

AI compliance for law firms: firm-level considerations

by *Shawn Curran* and Natalie Cooksey, *Travers Smith LLP*

Practice notes | **Maintained** | England, Wales

A note discussing the firm-level compliance issues that SRA regulated law firms should consider when using artificial intelligence (AI) (including generative AI) and legal technology tools, both within their business and in the provision of legal services.

Scope of this note

Artificial intelligence (AI) allows computers to perform tasks that would normally involve human intelligence. Machine learning is a type of AI through which computers identify and learn from patterns within data (for example, to answer questions posed by the user), as opposed to being programmed to produce a particular output (see *Practice note, AI jargon buster*).

AI can be viewed in two categories:

- Legacy AI includes basic entity extraction and classification, such as detecting certain clauses within a contract.
- New AI includes new, transformer-based large language models that can carry out more complex cognitive tasks, such as assessing the language the customer uses in emails to predict the likelihood of the customer terminating an agreement.

The development of new AI effectively moves the technology closer to a position where it can understand concepts and draw inferences in a more human-like manner.

Reflecting a greater willingness among clients and consumers to engage with AI systems and legal technology tools, many law firms are increasingly looking to harness the benefits of such technology, both in managing their businesses and in providing legal services.

However, use of these tools creates risk and law firm risk and compliance professionals must ensure that their firm's deployment of AI (particularly new AI) is safe for their business and clients and is in line with relevant legal and regulatory obligations.

This note examines the regulatory and compliance issues that firms should consider at firmwide level when using AI and legal technology in their business. It focuses on issues that would be of concern to the firm's risk and compliance professionals and does not cover wider legal considerations arising out of the use or development of AI tools (for example, employment law or product development issues).

The note is aimed at SRA regulated law firms practising in England and Wales but will also be of interest to other legal services businesses.

The Legal Services Board has issued guidance to regulators on how they should ensure that their regulatory approach to AI use in their regulated communities encourages innovation and aims to widen consumer access to justice (*LSB: Guidance on*

promoting technology and innovation to improve access to legal services. The SRA's approach may therefore develop over time. We will update this resource when further information becomes available.

For information about the key overarching regulatory duties, and the client and matter-level issues, that law firms should consider in relation to their use of AI and legal technology, see Practice notes:

- *AI compliance for law firms: key considerations.*
- *AI compliance for law firms: client and matter considerations.*

Supply chain compliance

Due diligence

If the firm intends to engage a third-party provider of AI or legal technology services, the firm should carry out appropriate due diligence on that provider to ensure that they are an appropriate organisation to work with.

Factors to consider include:

- Whether the provider aligns with the firm's outlook on environmental, social and governance (ESG) issues.
- Whether the provider is financially stable, bearing in mind the fact that many organisations in this sector are tech startups.
- The jurisdiction in which the provider is based.

The firm may wish to carry out detailed checks on the provider's information security arrangements. One way to do this is by sending the provider an information security questionnaire covering topics such as:

- How data uploaded to the platform will be secured.
- Where it will be hosted.
- Who will have access to the data once uploaded.
- Whether any sub-processors will be involved in handling the data.

The provider's answers to these types of questions will assist the firm in completing a comprehensive impact assessment (see *Practice note, AI compliance for law firms: key considerations: Data protection impact assessment*).

Contract review

The firm should ensure that any contract with the third-party provider is properly reviewed from a legal perspective, with appropriate consideration of issues such as governing law and risk and liability allocation (including the appropriateness of indemnities to cover the risk of intellectual property (IP) infringements arising from any output generated by the system). There should also be a requirement for the third-party provider to carry appropriate insurance.

For more information on how to approach contracting with third-party suppliers in this sector, see [Checklist, Contracting for AI: anatomy of an AI project](#) and [Article, AI governance, risk and compliance: shaping an unknown future: AI platform contracts](#).

In particular, the firm should be cautious of agreeing to a contractual provision that allows the provider to terminate the contract for convenience, especially where this might lead to significant business disruption to the firm (see [Business continuity](#)).

AI-powered system upgrades

Some of the firm's usage of AI may arise through existing suppliers introducing new AI-powered versions of their products, such as Microsoft's introduction of its Copilot AI tool. If the firm intends to subscribe for AI-powered features, it should update the impact assessment for the relevant product or service. Where personal data will be processed by the system, the firm should consider its transparency obligations towards any affected data subjects.

The SRA has confirmed that:

"If there is an error or flaw in an AI system run, or provided by, a separate technology company then [the SRA is] unlikely to take regulatory action where the firm did everything it reasonably could to assure itself that the system was appropriate and to prevent any issues arising." (See *SRA: Technology and legal services (11 December 2018)*.)

Therefore the firm should keep records of the steps taken as part of its procurement or upgrading process, alongside details of any testing carried out (see [Practice note, AI compliance for law firms: key considerations: Monitoring and controls](#)).

Keep in touch with existing suppliers

Third party technology providers who sit above base model vendors such as Google and Microsoft, and who are looking to incorporate AI tools into their offerings, appear increasingly keen to be able to use data uploaded into their systems to train their proprietary models.

Law firms should resist this and be alert to the issue when reviewing supplier contracts. It is best practice to keep in touch with existing software suppliers on an ongoing basis about their intentions regarding their use of AI, to ensure that the firm does not get caught out by suppliers turning on any AI functionality without the firm's knowledge and consent.

Business continuity

If the firm is reliant in any way on an AI system, it should put in place detailed service level agreements with the relevant providers, as well as internal plans addressing how the firm will deal with any outage or compromise of the system. The firm should document these plans as part of its business continuity procedures and cyber incident response arrangements.

Pursuant to the requirement to act with independence under Principle 3 of the [SRA Principles](#), the firm must ensure that its relationship with any third-party technology provider does not compromise the firm's independence. The firm should therefore ensure that the contract with the provider enables the firm to easily extract its data, source code, and any existing training on the tool and switch to another provider, for example if a dispute arises or if there is a change of control to a new provider with whom the firm does not want to have a business relationship.

As far as possible, the firm may wish to consider conducting data-labelling processes (such as the tagging of certain types of clauses within a contract) outside of the AI system, to ensure this work product is not tied into the AI system.

For further information on AI supply chain considerations, see Checklists:

- [What to look out for in a LawTech implementation contract.](#)
- [Identifying and Selecting Compliance Software: A Step-by-Step Guide.](#)
- [Contracting for AI: anatomy of an AI project.](#)

Professional indemnity insurance (PII), panels and quality marks

PII insurers are taking an active interest in the way in which firms are proposing to utilise AI tools in the provision of services to clients. If insurers consider the firm's use of AI or legal technology increases the firm's risk profile, this may lead to increased PII premiums.

As insurers develop their knowledge of how firms are using and benefitting from AI, they may ask more searching questions at renewal about what controls firms have in place (if any) in relation to their use of AI systems and any potential impact on service standards and regulatory compliance.

The firm may face similar questions on re-accreditation of any quality accreditation marks, or on review of any panels of which the firm is a member (for example, lender panels).

Examples of the concerns that may be raised include:

- Asking whether firms are using "open" or "closed" AI models. Although there are other factors, the key distinction between these is that an open model uses data inputted into the system (including prompts) to learn and improve its output for the benefit of other, external, users, while a closed model learns only for the benefit of the firm's users.
- Wanting to understand how the firm is ensuring that any legal work product which incorporates AI output is accurate, of a suitable quality and has been appropriately supervised, so as to minimise the risk of a professional negligence claim.
- Requiring the firm to include specific provisions in its contracts with third-party suppliers of AI systems.
- Enquiring about the risk of confidentiality breaches arising from AI's iterative learning from the prompts inputted into the system. As such, it will be important to be able to demonstrate to insurers that appropriate procedures are in place to protect confidential client information.

Training

Rule 4.3 of the SRA Code of Conduct for Firms sets out a general requirement for firms to ensure that their managers and employees are competent to carry out their role and keep their professional knowledge and skills up to date. This is reflected in rule 3.3 of the SRA Code of Conduct for Individuals.

In relation to AI use in particular, the LSB guidance to regulators on how they should approach AI use in their regulated communities suggests that regulators might consider using ongoing competence requirements to encourage legal professionals to keep themselves up to date with developments in AI and legal technology and how they might be used to improve access to legal services (*LSB: Guidance on promoting technology and innovation to improve access to legal services*).

The firm should therefore consider appropriate staff training a key part of its AI compliance program.

Appropriate usage

Many firms have implemented AI use policies detailing how staff should, and should not, use AI in the course of their work for the firm. Any staff usage policy should clearly outline the extent to which employees are permitted to use AI tools to perform their work functions, alongside some examples of permitted use cases and the types of information that may be entered into the system.

It may also be prudent to put in place some firm-wide ethical principles or a values statement outlining how your firm intends to engage with AI. This could address issues such as the development of AI and the use (or prohibition of the use) of AI in recruitment, appraisal and promotion processes or for the purposes of automated decision making or profiling. For an example of a business code of conduct and ethics, and a generative AI usage policy, see Standard documents:

- [Code of conduct and ethics \(UK\)](#).
- [Generative artificial intelligence in the workplace policy](#).

The firm will need to communicate clearly with staff about any limitations on their freedom to explore and experiment with AI systems other than those the firm provides. While these technologies can drive huge efficiency savings, it is vital that the firm applies appropriate due diligence and risk management consideration to their procurement and development. Staff should be warned not to subscribe for “shadow” technologies that have not gone through the firm’s internal procurement processes. Where an AI or legal technology committee exists, the firm should ensure staff understand when requests for a new technology to be developed or onboarded should be routed to that committee for approval.

For further information, see [Article, AI governance, risk and compliance: shaping an unknown future: AI staff policies](#).

For an example of a policy relating specifically to the use of generative AI, see [Standard document, Generative artificial intelligence in the workplace policy](#).

Technical training

Staff training is essential to ensuring that any AI systems implemented by the firm are used safely and that users are aware of the risk of inaccuracies and biases in generative AI output. Staff will need to be trained on how to use the AI system properly, effectively and as safely as possible.

The firm should review and, if necessary, update its existing training courses in light of the firm's use of AI and the impact that that may have on the responsibilities of more junior lawyers (for example, how they might use AI for research or document analysis tasks).

The firm may also wish to encourage staff to attend external technology events and seminars, to ensure that they are up to speed with any legal technology developments that could benefit the firm or its clients.

The firm should keep records of the training given to end-users on how to use the technology in an appropriate way.

In any use of AI or legal tech systems, practitioners should be mindful of their obligations under rules 3.2 and 3.5 of the SRA Code of Conduct for Individuals, and that they remain responsible for the work they and those they supervise carry out for clients, regardless of whether they have been assisted in that work by AI technology.

For further information about staff AI training, see:

- [Video, *Legal technology: developing legaltech skills within your firm.*](#)
- [Standard document, *Generative AI in the workplace \(UK\): training materials.*](#)

Staff issues

Succession planning

As part of succession and future planning, the firm should consider whether it needs to adapt its approach to recruitment to focus on new skillsets for an AI-enabled legal profession. As the role of legal technology becomes more prevalent and more repetitive tasks start to be performed by AI systems, the organisational structures of law firms may change, with a greater focus on recruiting into the technology department and a need to recruit staff (both operations and legal staff) who have an interest in, and experience of, AI and legal technology systems.

Recruitment and appraisal systems

Firms and practitioners are required to:

- Treat colleagues fairly and with respect.
- Not discriminate unfairly against colleagues.

(Rule 1.6, SRA Code of Conduct for Firms and rule 1.5, SRA Code of Conduct for Individuals.)

If the firm is considering using AI systems in its staff recruitment, appraisals or other staff management processes, the firm will need to consider how it will ensure that its usage complies with these requirements. This may involve examining the data on which the AI system is trained to assess whether this is likely to introduce any biases or other unfairness into the system. For example, if recruitment system training data only included candidate examples who obtained GCSEs, the system may disregard candidates with other equivalent qualifications, which may itself lead to biases including, for example, in relation to nationality or age.

The firm should ensure that appropriate information is given to prospective and current employees (as applicable) about:

- The firm's use of AI tools in these processes.
- The extent of any automated decision-making or monitoring.
- The extent to which the AI is supervised by humans.

The information should include details of any right of review or right to request purely human decision making.

For further information, see *Practice note, AI in the workplace (UK)* and *ICO: Rights related to automated decision making including profiling*.

Human resourcing

When AI and legal technology tools are effectively improving processes and reducing inefficiencies within a firm, this may impact on the firm's overall staffing needs, both in terms of required staff numbers and work types or roles. For example, it is possible that, in the future where an AI system has been fine-tuned to understand complex concepts within a specialist area, it may be able to reason as effectively as a human lawyer, thereby negating the need for processes commonly currently undertaken by junior lawyers or paralegals, such as a first-level document review.

The firm may wish to engage with AI as an asset that augments the capabilities of human lawyers, rather than as a system that can be used to replace them.

As with all change management initiatives, the firm should plan for any changes it wishes to make to existing staff roles occasioned by the firm's use of AI and should take specialist legal advice if needed.

For further information about law firm change management, see *Practice note, Change management: an introduction*.

Intellectual property (IP) issues

The firm's IP

The use of large language models can pose a significant risk to an organisation's IP rights. Where material that belongs to a firm is uploaded to an open or consumer version of an AI model (for example, ChatGPT), that material may be used to further train the model and to inform the model's responses to prompts from users outside the organisation. For this reason, the firm must make clear to staff in its user policies (see *Staff issues*) that the firm's IP must not be uploaded into AI systems.

The safest approach is to use an enterprise version of the software, which does not permit any data that is uploaded to the system to be used for the purpose of training the model, and by ensuring that all data used to fine tune the model is appropriately cleansed before use.

Third-party IP

There is a risk that models that have been trained on publicly available data could have collected that data in breach of a website's terms of use (given that many websites' terms of use seek to prohibit web-scraping) or could generate output that incorporates IP belonging to an external third-party organisation, causing the firm's use of the output to breach the third party's IP rights. Although the latter risk may be remote, it is one that has been expressly acknowledged by technology companies, with Microsoft and OpenAI both going so far as to offer their customers an indemnity in respect of IP infringement claims arising from the use of output generated by their AI systems. The risk of third-party IP breaches is therefore another reason why all output should be checked by a human supervisor before onward use.

Risks of development

Taking the above into account, the firm should consider whether it is comfortable investing time and resources into developing an AI model in circumstances where base model owners are facing copyright claims and investigations from data protection regulators. As content creators mount legal challenges to their historic data having been scraped by AI bots, and seek to prevent

new content from being used in this way, there is a risk of model deterioration until questions around how content creators ought to be properly remunerated, and how personal data can be fully extracted from models, are determined.

Developers' IP

When commissioning an AI system to be built by a developer, the firm should ensure there is no confusion between the firm and the developer about the ownership of the IP in any content produced by the system, including any rights in improvements in the AI which result from training data. The firm should consider whether to take specialist legal advice on the issue and should ensure it is expressly addressed in the firm's agreements with their third-party developers and providers of AI systems.

For further information, see [Checklist, Artificial intelligence and copyright](#).

Further reading

For further Practical Law resources on the use of AI and particular issues for law firms, see:

- [Legal technology and artificial intelligence toolkit](#).
- [AI toolkit \(UK\)](#).

| |
|-----------------|
| END OF DOCUMENT |
|-----------------|