

CURRENT GUIDANCE

Valid from 18 May 2026

Guidance on the use of Artificial Intelligence and Other Technologies

Introduction

The BSB supports the adoption and use of technologies, including Artificial Intelligence (AI), where they are likely to benefit practice management, or the availability, quality or client experience of barristers' services. At the same time, effectively procuring, adopting, and using technologies takes skill and resources, so you should prepare appropriately.

This guidance is issued primarily to address the risks posed by Generative AI tools as used within the legal services professions since their development. However, the principles underlying this guidance apply to the use of any technology.

Structure of this guidance

This guidance is organised by stage of AI adoption and use, rather than by order of importance. It first addresses the competence and practice management responsibilities relating to AI adoption before addressing responsibilities at the immediate point of use. It covers:

1. **General ethical considerations** – BSB Handbook responsibilities that apply at all times when using AI and other technologies
2. **Using technology competently** – Ongoing training and competence standards, including continuing professional development (CPD)
3. **Before adopting a new technology** – Practice management and chambers management standards when acquiring AI systems and other technologies
4. **Setting technology management and use procedures** – Practice management and chambers management standards governing appropriate use
5. **Each time you use AI, and duties to clients** – Responsibilities at the point of use, and duties when using AI to support client work
6. **Your responsibilities when others use AI** – Responsibilities when solicitors, clients, and others you work with use AI

1. General Ethical Considerations

The use of AI and other technologies engages many of the ethical principles and Core Duties underlying the BSB Handbook. When considering whether and how to use technology in your legal practice, you should consider how it will impact your ability to fulfil the Core Duties and rules within the BSB Handbook. The following Core Duties and rules are likely to be engaged at multiple stages over the course of AI adoption:

Core Duty 7: You must provide a competent standard of work and service to each client. You should maintain a sufficient level of competence in technology and AI to understand how they may impact your practice, whether or not you adopt those technologies yourself. For example, you should understand the benefits and risks of technologies that may be adopted by opposing counsel or clients, and the changing status of AI under court practice¹ and the law². Emerging themes in this area include considering and being able to detect the potential for error in AI-generated submissions, identifying when legal professional privilege may be compromised by clients or professionals using AI systems, and the admissibility of AI-generated evidence and prompt histories.

Before using AI or other new technologies, you should ensure you have a level of competence in how the technology functions, sufficient to understand how to operate it safely, and how to incorporate it effectively into your practice.

Core Duty 2: You must act in the best interests of each client. Before using AI in a matter, you should consider whether it is in the best interest of the client to do so. You may consider how your client would benefit from your use of an AI tool rather than an alternative approach, and at what cost or risk to them, in determining whether and how to proceed.

Core Duty 3: You must act with honesty and with integrity. You should ensure you are able to maintain honesty and integrity when using AI or other technologies. You must be transparent about your use of AI tools, especially if asked by your client, the court, or the BSB, if it materially impacts the nature and scope of your legal service, and if required under UK law (e.g. GDPR) or court practice rules. You must not knowingly or recklessly mislead your client (rC19) or the court (rC3) through your use of AI. This includes ensuring any work you carry out using AI is accurate, and being clear and accurate about the nature of the services you provide, including whether they were carried out using AI.

Personal responsibility for your work (rC20) and outsourcing (rC86). You are personally responsible for your own conduct and your own professional work, including when using AI tools. You should be able to justify your decisions and actions, and you must be transparent about your use of AI when asked by a client or the court. Any inaccuracies introduced through the use of AI or other technologies remain your responsibility. Using AI and other technologies amounts to outsourcing under rC86, therefore you remain responsible for your work and for compliance with BSB obligations when using AI (rC86).

¹ See for example: *Artificial Intelligence (AI) Guidance for Judicial Office Holders*. Courts and Tribunals Judiciary (31 October 2025). <https://www.judiciary.uk/wp-content/uploads/2025/10/Artificial-Intelligence-AI-Guidance-for-Judicial-Office-Holders-2.pdf>.

² See for example: *Artificial Intelligence and the Law: a discussion paper*. Law Commission (31 July 2025). <https://lawcom.gov.uk/publication/artificial-intelligence-and-the-law-a-discussion-paper/>. And, the UK Jurisdiction Taskforce public statements: <https://lawtechuk.io/ukjt/>

Core Duty 10: You must take reasonable steps to manage your practice, or carry out your role within your practice, competently and in such a way as to achieve compliance with your legal and regulatory obligations. You should ensure you are able to procure and manage AI technologies competently and efficiently as part of your general practice and chambers management responsibilities (rC87.1, rC89). You may wish to consider appropriate frameworks and governance structures prior to adoption of new technology to ensure you and your organisation are prepared to manage AI systems and risks they may pose, for example AI assurance³. Prior to procuring an AI system or other technology, you must ensure it is able to fulfil the confidentiality and personal data processing responsibilities you hold under the BSB Handbook (Core Duty 6, rC86), court procedure, and UK law (e.g. GDPR). You should ensure you have adjusted its settings to comply with these responsibilities and keep proper records (rC87.2), which may include AI audit logs and appropriate prompt histories. You should ensure any existing data policy you or your chambers maintain is adapted if necessary to cover AI use, and consider establishing an AI policy, to include acceptable uses, record keeping procedures, data governance and AI governance procedures, prior to using AI tools in your practice.

Core Duty 1: You must observe your duty to the court in the administration of justice. You have a duty to the court to act with independence in the interests of justice (rC3, rC4). You must ensure any use of AI does not contravene this duty, for example by ensuring you do not knowingly or recklessly mislead the court about, or as a result of, your use of AI (rC3, rC6). You should be aware of the Judicial Guidance on AI, including the expectations on judicial office-holders regarding how to handle the use of AI by legal representatives⁴. The Judicial Guidance currently states: “Provided AI is used responsibly, there is no reason why a legal representative ought to refer to its use, but this is dependent upon context.” The Hamid jurisdiction judgment in the *Ayinde* and *Al-Haroun* cases⁵ sets out further expectations of legal representatives when using AI, and you should have regard to this judgment and any future case law on this matter.

Core Duty 8: You must not discriminate unlawfully against any person. AI systems generally tend to exhibit bias in their outputs in relation to protected characteristics in a way that reflects bias in the data they are trained on⁶. You should be aware of this likelihood, design your interactions with the tool in such a way as to minimise bias (e.g. removing indicators of protected characteristics in your prompts), verify outputs through independent sources, and consider alternative methods of corroborating findings and their implications in your work⁷. Such bias is likely to impact the accuracy of AI outputs and therefore their

³ e.g. *Introduction to AI Assurance*. Department for Science, Innovation & Technology (12 February 2024). <https://www.gov.uk/government/publications/introduction-to-ai-assurance/introduction-to-ai-assurance>

⁴ *Artificial Intelligence (AI) Guidance for Judicial Office Holders*. Courts and Tribunals Judiciary (31 October 2025). <https://www.judiciary.uk/wp-content/uploads/2025/10/Artificial-Intelligence-AI-Guidance-for-Judicial-Office-Holders-2.pdf>

⁵ [2025] EWHC 1383 (Admin). <https://www.judiciary.uk/wp-content/uploads/2025/06/Ayinde-v-London-Borough-of-Haringey-and-Al-Haroun-v-Qatar-National-Bank.pdf>

⁶ See for example: <https://www.ucl.ac.uk/news/2024/dec/bias-ai-amplifies-our-own-biases>

⁷ Consider for example ICO guidance on fairness, bias, and discrimination impacts of AI and proposed mitigations for organisations using AI: *What about fairness, bias and discrimination?* Information Commissioner’s Office. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-fairness-in-ai/what-about-fairness-bias-and-discrimination/#risks>

reliability. You should also take extra caution when using AI tools for areas of law likely to correlate with vulnerability or particular protected characteristics (e.g. immigration and asylum).

This bias may also lead to unlawful direct or indirect discrimination in contravention of the Equality Act 2010, if not recognised and mitigated (rC12).

A risk-based approach

We encourage you to take a risk-based approach to technology adoption and use, satisfying yourself that you have identified and can manage the risks and costs a particular technology for a particular use may pose, and that the benefit it presents in that situation outweighs those risks. You should take appropriate steps to manage the risk, having regard to this guidance, ongoing developments in the legal technology space, and general standards for AI governance and risk management⁸.

Barristers should be able to demonstrate they have taken a reasonably active and informed approach to managing technology risks, proportionate to the risk or harm (*Core Duty 10*). Risk may arise from the **application** (i.e. the intended outlet for the tool output, including the area of law and characteristics of your client), the **use** (i.e. the manner in which you use the tool), and the **technology** itself (i.e. the specific tool you use). We encourage you to consider the interactions of these three factors in determining whether it is safe to proceed, the degree of competence you may require for safe use, and what risk mitigations may be necessary.

	Likely low risk	Likely medium risk	Likely high risk
Application	Administrative uses for improved client experience (e.g. meeting reminders)	General client work or preliminary research, work with sophisticated clients	Court submissions, work with vulnerable clients, areas of law likely to correlate with certain protected characteristics or vulnerability
Use	Spelling/grammar, minor text edits, certain general administrative tasks	Legal research	Text generation, drafting, automated/agentive features
Technology	Spelling/grammar tools with sufficient data protection or used on non-sensitive documents	Legal-specific AI tools, general purpose generative AI tools within secure environment	Agentive AI, general purpose generative AI tools without adequate data protections

⁸ See for example: *Artificial Intelligence*. British Standards Institution. <https://www.bsigroup.com/en-GB/our-expertise/digital-trust/artificial-intelligence/>
ISO/IEC 42001 AI Management System. International Standards Office. <https://www.iso.org/standard/42001>

2. Competent use of technology

We encourage all barristers to maintain a basic level of general technology and AI competence, to understand how it may impact your practice even if you do not use the technologies yourself.

You should maintain a basic level of competence in technology and to stay up to date on developments in both the general and legal-specific technology environments. A basic level of competence in technology includes an awareness of relevant technology available to support legal practice and the benefits and risks of general technologies that may impact your practice, for example those adopted by opposing counsel or clients. This is because general technology competence supported by good AI and data literacy will help you to:

- stay aware of changing professional practice norms,
- recognise and adapt to the impacts on your practice of technologies used by clients, solicitors, the courts, or opposing counsel
- recognise the possibility that any tools you already use may change to incorporate AI (including web search tools and text editing software), and
- identify opportunities to adopt technologies that advance your clients' interests.

Even where you do not adopt AI technologies, we encourage you to be aware of its changing impacts on the law and status in the courts. For example, you should be conscious of the validity and admissibility of AI prompt histories and AI-generated evidence, client documents, and opposing parties' submissions⁹.

<i>Why we're interested:</i>	This expectation derives from: Core Duty 7 (Competent standard of work), Core Duty 10 (Practice management), ongoing competence expectations and CPD obligations.
<i>Key competencies engaged</i>	Professional Statement 1.12. All barristers should be able to identify the legal and non-legal issues relevant to a matter, which includes being able to identify and appropriately respond to uses of AI by clients, instructing solicitors, and opposing counsel, and to understand any changes in the treatment of AI and other technologies under the law and court procedure.

You should be competent in the use of technology tools and AI that you adopt.

When adopting new technologies and innovations, you should ensure you are sufficiently competent to understand how the technology functions, how to operate it safely, and how to incorporate it effectively into your practice (rC86.3). In the case of generative AI technologies, this means you should understand:

- how the tool was created and trained (e.g. the scope of data it was trained on, inclusion of legal-specific information, any date or jurisdiction limitations),

⁹ See for example *Oakley v Information Commissioner* [2024] UKFTT 315 (GRC)

- what it does and does not do (predictive text generation, searching capabilities, explainability of results, confidentiality of inputs or prompts, etc), and
- what it can provide (veracity, legal validity, etc)

You should understand these points sufficiently well to ensure you can mitigate any additional risks it creates as compared with what you would have done without the technology.

<i>Why we're interested:</i>	This expectation derives from: Core Duty 1 (Duty to the Court), Core Duty 2 (Best interests of each client), Core Duty 6 (Confidentiality), Core Duty 7 (Competent standard of work and service), Core Duty 10 (Practice Management)
<i>Key competencies engaged</i>	Professional Statement 1.5, 1.6, 1.10 and 1.12. Barristers using AI for legal analysis should have sufficient skill in using these tools, understand how to methodically evaluate the quality and reliability of their outputs, and apply legal principles to outputs to reach reasoned decisions.

3. Before adopting a new technology

*We encourage you to **evaluate the benefits, risks, and costs of new technologies before adopting them**, including the specific uses you are likely to carry out.*

Prior to adopting or using a specific tool, you might consider the general problem you aim to address and setting out the ways in which technology adoption or other changes may respond to that problem. You may consider drafting a “business case”¹⁰ for adoption, in which you define the need and criteria for assessing potential solutions, or making a change management plan and a list of alternative tools prior to procurement. You should also consider what training or competence you may need to use the new technology effectively, how it will impact your work, risks or limitations it presents, and whether it is an appropriate or cost-effective means of achieving the intended need.

You should generally consider the benefits, risks, contractual terms, and costs of each tool you consider adopting; this is especially important with respect to the security of your client data. You should also consider what recourse you and/or your clients may have if something goes wrong, and what may happen to any data or funds if you cease to use the tool or if its provider goes out of business or ends support for the tool.

<i>Why we're interested:</i>	This expectation derives from Core Duty 10: <i>You must take reasonable steps to manage your practice, or carry out your role within your practice, competently and in such a way as to achieve compliance with your legal and regulatory obligations.</i>
------------------------------	--

¹⁰ See for example: https://en.wikipedia.org/wiki/Business_case

<i>Key rules engaged</i>	rC87/rC89. Considering the factors listed above, and/or developing a business case, for your use of AI will help demonstrate you have managed your practice/chambers efficiently and competently.
--------------------------	--

You must consider the **client confidentiality and data security** impacts of any tool you procure.

You must ensure any tool you adopt will not compromise your ability to satisfy your client confidentiality requirements under the BSB Handbook (Core Duty 6), any confidentiality obligations you may have to the court, and any obligations you may have as a data controller or processor under UK GDPR. You should also consider whether any tool you use should be certified or should comply with the ICO Legal Services Operational Privacy Certification Scheme (LOCS) standards. You should also consider whether any data storage, handling, or processing occurs outside the United Kingdom and whether this international data transfer is acceptable under those obligations listed above¹¹.

<i>Why we're interested:</i>	This expectation derives from Core Duty 6 (Confidentiality), and rC86-89
<i>Key rules engaged</i>	<p>rC86.3. The use of AI tools constitutes outsourcing a support service for the purposes of rC86, whether used for legal or administrative work. You must ensure any technology you procure can maintain your confidentiality obligations under the BSB Handbook and process any personal data in accordance with your instructions, both in terms of technical capability and its contractual terms of use.</p> <p>rC87/rC89. You must ensure any technology you introduce into your practice does not compromise client confidentiality requirements as part of your requirement to manage your practice/chambers efficiently and competently.</p>

4. Setting technology management and use procedures

You should ensure IT systems are appropriately implemented.

You must ensure you have adequate data access restrictions on any technology you implement to ensure you can comply with your client confidentiality obligations (Core Duty 6, rC86). You should consider any data access or privacy settings governing the technology provider or third parties' access to data, prompts, documents, or other

¹¹ The Bar Council IT/UK GDPR guidance provides a set of relevant considerations when procuring and using any technology, including AI, especially those that involve third party storage or processing (e.g. cloud computing). <https://www.barcouncilethics.co.uk/subject/it/>

information (including for model training, product development, marketing, error handling, or other reasons), as well as access settings on any shared systems (e.g. within chambers).

You should also consider the level at which an AI system aggregates and learns from user inputs or prompts, particularly if implementing the system at chambers- or entity-level. For example, if building a custom AI assistant or custom GPT, you should ensure it is configured appropriately to secure the prompts and information you enter. In this case, you should consider the risk that other barristers in chambers (for self-employed barristers), or other teams in your entity/employer (for BSB entities, employed barristers) may be able to view or infer sensitive client information (based on your input data or your prompts), particularly if other barristers in your chambers are representing an opposing party.

You should be especially cautious if using a general-purpose and/or free generative AI tool, as terms of use typically enable the technology providers to claim ownership or rights to any input data or prompts, store them indefinitely, and use them to train their model. These terms may in turn enable other users to infer sensitive client information if they ask closely relevant prompts. These tools will usually be too high risk to use for legal work or client-specific tasks, including practice management tasks, and you should generally only use them for the lowest risk applications, if at all. Such uses may include learning about AI, general administrative work not tied to a specific client, or general training exercises (e.g. training pupils to prepare for cross-examination) that do not involve actual case details.

<i>Why we're interested:</i>	This expectation derives from Core Duty 6 (Confidentiality)
<i>Key rules engaged</i>	rC86. The use of AI tools constitutes outsourcing a support service for the purposes of rC86, whether used for legal or administrative work. Your use of AI does not alter your obligations to your client, and you remain responsible for compliance with your obligations under the BSB Handbook in respect of the legal services provided when using AI tools. You should ensure the terms of your use of AI systems (i.e. with the AI system provider) fulfil the conditions set out in rC86.3. It is unlikely that free-of-charge, publicly available AI systems fulfil these conditions.

*You should consider **setting data governance and AI governance policies and procedures** to ensure you can operate AI and other technologies safely in your practice.*

As part of your practice management and chambers management responsibilities, you should be able to set out how you will use AI or other technologies, what constitutes acceptable use, and what procedures you put in place to ensure your use of the technology is compliant with BSB regulations and your other legal obligations. You may need to conduct this exercise at both the individual and chambers/entity-levels. What constitutes safe use depends on the sensitivity and risk of how you plan to use the technology. You should consider the following governance procedures:

- drafting an explicit AI governance policy, particularly when implementing AI systems at chambers-level for use by multiple barristers and staff members
- tailoring the tool settings appropriately for how it is to be used
- setting data and prompt deletion policies and establishing AI audit logs that demonstrate the process you used to generate the outputs you rely on in your work

<i>Why we're interested:</i>	This expectation derives from Core Duty 6 (Confidentiality) and rC86-89
<i>Key rules engaged</i>	<p>rC87/rC89. Setting appropriate policies and procedures will help you demonstrate that your practice and your chambers are efficiently, competently and properly administered.</p> <p>In particular, you should ensure your AI system is set up to allow you to retain all appropriate records, which may include enabling AI audit logs, data and prompt deletion policies, particularly where using AI for client work.</p>

When adopting an AI tool, we encourage you to consider in general how you intend to use the tool, and how it will comply with your own AI policies (as above) and broader obligations.

Some questions to consider are:

- what aspects of your work will you use AI for and how well suited the tool you use is likely to be for that task (e.g. administrative work, communications, legal research),
- what applications or uses are acceptable and unacceptable,
- what risks might the AI tool pose when used for those purposes and how you will manage these,
- how you will verify and validate AI outputs, and
- how you will incorporate its outputs into your practice for the intended task.

You may consider creating a 'playbook'¹² or 'standard use procedure' that sets out what you will and will not use AI for, how you will do so, and how you will verify its outputs when incorporating them into your work. This is especially relevant when adopting tools at the chambers level.

<i>Why we're interested:</i>	This expectation derives from Core Duty 10: <i>You must take reasonable steps to manage your practice, or carry out your role within your practice, competently and in such a way as to achieve compliance with your legal and regulatory obligations, and responsibilities to manage your practice efficiently and competently under rC87/rC89.</i>
------------------------------	--

¹² As an example of what form this may take, consider the Government Digital Service [AI Playbook for the UK Government](#). While this document and its procedures are more detailed than necessary for barristers' use, the principles, structure, and certain governance procedures may be a useful model.

5. Each time you use AI, and duties to clients

You remain responsible for your work at all times when using AI or other technologies.

You are ultimately responsible for your work when using AI or other technologies, especially when using such technologies for legal work on behalf of a client or for submissions to the court (rC20). You must ensure any outputs from AI systems are accurate and appropriate for the intended use before including them in your work, due to your obligation not to knowingly or recklessly mislead anyone (rC9.1) and not to mislead the court (rC3). You generally should not copy AI output directly into your work product, rather you should review such output for accuracy and applicability and adapt it appropriately to your work.

Agentic AI features, which allow an AI system to take an action automatically based on its output, are likely to be of high risk for most applications at the Bar and should be considered with absolute caution. It may be appropriate and desirable to automate certain low-risk administrative tasks (e.g. allowing case management software to automatically generate reminder emails to clients for appointments or about missing documents, or capturing updates about public documents on the internet), but you should maintain strict controls on how such automations are carried out because you remain responsible for any actions such a system may take (rC20, rC86.3.b).

<p><i>Why we're interested:</i></p>	<p>This expectation derives from Core Duty 5 (Trust and Confidence in your or in the profession), Core Duty 7 (Competent Standard of Work), Core Duty 10: <i>You must take reasonable steps to manage your practice, or carry out your role within your practice, competently and in such a way as to achieve compliance with your legal and regulatory obligations</i>, and responsibilities to manage your practice efficiently and competently under rC87/rC89</p>
<p><i>Key rules engaged</i></p>	<p>rC9. You should not incorporate AI outputs into your work without independently verifying their accuracy and appropriateness. Reliance on AI systems without carrying out standard legal research processes may breach rC9.1 (recklessly misleading) or .2 (statement of fact not supported by instructions or any contention which you do not consider to be properly arguable).</p> <p>rC20. You must use your own professional judgment at all times when using AI, or other technologies, and be able to justify your decisions and actions. You must ensure any work you carry out is accurate and appropriate, which typically will require reviewing and adapting any AI outputs you use as part of a discrete task.</p>

When using AI for client work, you must act in *the best interests of each client (CD2)*, provide a *competent standard of work and service to each client (CD7)* and keep the *affairs of each client confidential (CD6, rC15)*.

You should ensure that your use of AI in a particular instance, the prompts you use, and the way you incorporate AI outputs into your work is in the best interest of your client, is carried out competently, and is secure. You may consider how your client would benefit from your use of an AI tool rather than an alternative approach, and at what cost or risk to them, in determining whether and how to proceed.

<i>Why we're interested:</i>	This expectation derives from Core Duty 2 (Best interests of each client), Core Duty 5 (Trust and Confidence in your or in the profession), Core Duty 7 (Competent Standard of Work)
------------------------------	--

You must ensure your use of AI adheres to *court practice rules and other professional or legal responsibilities*.

You must consider potential risks to legal professional privilege where disclosure of client information may impact court proceedings¹³. You must also consider potential risks regarding contempt of court for breaches of court procedure rules related to AI use, for example due to false information or disclosure of court proceedings¹⁴ (Core Duty 6). These responsibilities are adjudicated by parties other than the BSB (e.g. the Judiciary) and may result in harms and penalties beyond professional sanction. You must also ensure your use of AI tools complies with GDPR and other regulations, including appropriate handling of client data, disclosure to clients under GDPR, and ensuring the AI systems you use allow you to comply with any recourse clients may have under GDPR as to how their data is handled¹⁵.

<i>Why we're interested:</i>	This expectation derives from Core Duty 1 (Duty to the Court) and Core Duty 10 (Practice Management).
<i>Key rules engaged</i>	<p>rC15. Use of client data or personally identifiable information in AI tools may breach your obligation to protect the confidentiality of your client's affairs if you do not use appropriate safeguards.</p> <p>rC86. You must ensure that any processing of personal data by a third-party software does so in accordance with your responsibilities and complies with data protection laws.</p>

¹³ Please see the decision in *UK and R (on the application of Munir) v Secretary of State for the Home Department* [2026] UKUT 81 (IAC), which addresses legal professional privilege implications of AI use. For example, at 4, "Uploading confidential documents into an open-source AI tool, such as ChatGPT, is to place this information on the internet in the public domain, and thus to breach client confidentiality and waive legal privilege."

¹⁴ Please see the decision in *Ayinde v London Borough of Haringey* [2025] EWHC 1383 (Admin) for further consideration of the contempt of court implications of AI system use.

¹⁵ For example, you should consider the ICO resources on AI and GDPR: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/>

*You should consider the **accuracy of AI systems you use.***

It has been well documented that AI systems are likely to generate false citations when asked a legal question. This is because of how such systems operate – a generative AI system generates the most likely satisfactory sequence of text in response to a user prompt based on text patterns in its training data, and it recognises that relevant texts typically include numbers, letters, and names in the form of a citation.

However, false citations are indicative of a more general risk of accuracy. AI systems do not go through the same process that trained legal professionals would do, therefore you should not assume that an AI-generated summary or response has followed a particular reasoning approach or has considered all relevant information. AI tools may not accurately identify what the most important aspects of a case are from a legal reasoning (rather than a text prediction) standpoint. Legal-specific AI tools are likely to be of higher reliability than general purpose AI tools, because they are trained on legal data and case law and have been developed with features relevant for legal applications (e.g. checking citations), but you should not rely upon these assurances in full and should verify any references or conclusions via independent alternative sources¹⁶.

You must be transparent about your use of AI with your client if it materially impacts the nature or scope of your legal service (rC19).

You must act with honesty and with integrity (CD3) and are generally required to ensure clients and potential clients know what to expect and understand the nature and scope of the legal services you are offering (rC19). Where your use of AI materially impacts the nature of your legal service (i.e. as compared with the general standard of practice or with alternative means of achieving the desired outcome), you should take steps to ensure clients and potential clients understand this impact and any risks it may pose.

Further, if you are using AI, you should be familiar with the principle of transparency as it applies to data protection and AI¹⁷, including proactive obligations when processing data and best practices around responsible disclosure.

We encourage you to consider generally whether it is in your client's best interests or the court's interests proactively to inform your client or the court of your use of AI tools. In many circumstances, such disclosure may not be strictly required under UK law (e.g. GDPR) or court practice rules, as the recent Judiciary AI guidance indicates¹⁸.

If your use does not materially impact the nature or scope of your legal service, it may not be necessary to inform the client of this work, particularly if doing so may confuse

¹⁶ Legal-specific AI tools still demonstrate non-negligible rates of hallucination and inaccuracy: <https://hai.stanford.edu/news/ai-trial-legal-models-hallucinate-1-out-6-or-more-benchmarking-queries>

¹⁷ See for example: *How do we ensure transparency in AI?* Information Commissioner's Office.

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-transparency-in-ai/>

"Principle (a): Lawfulness, fairness and transparency". Information Commissioner's Office.

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/lawfulness-fairness-and-transparency/#transparency>

"Transparency and explainability (Principle 1.3)". OECD.AI Policy Observatory.

<https://oecd.ai/en/dashboards/ai-principles/P7>

¹⁸ <https://www.judiciary.uk/wp-content/uploads/2025/10/Artificial-Intelligence-AI-Guidance-for-Judicial-Office-Holders-2.pdf> at §VI

the client about the nature of your service. This may be the case where technology is used for low-risk administrative tasks or minor editing of non-sensitive documents, does not involve specific details about the client’s matter, and does not factor directly into your reasoning or work product.

But transparency is especially relevant in higher risk situations, for example to communicate how sensitive client information is handled when using client data or details of a matter within an AI system.

This is an opportunity to improve trust and confidence in the profession by helping clients better understand the process you will carry out. While you may not be required to disclose de minimis use of AI tools in general circumstances, you must respond honestly and transparently to any BSB or court enquiries about such use where the question arises in regulatory or court proceedings.

<p><i>Why we're interested:</i></p>	<p>This expectation derives from Core Duty 3 (Acting with Honesty and with Integrity), Core Duty 5 (Trust and Confidence in you and in the profession), and Core Duty 9 (You must be open and co-operative with your regulators)</p>
<p><i>Key rules engaged</i></p>	<p>rC19. You must be transparent about your use of AI or other technologies to clients when the use of that technology materially impacts the nature or scope of your service (rC19.1) or where it impacts who is legally responsible for the provision of services (rC19.3). For example, this is likely to be the case if you plan to use AI as an integral part of your work or to do things you would not otherwise do by alternative means, if the client’s data will be processed by another party, or if the client may have recourse to another party if something goes wrong. You must ensure your client is not misled about the nature of your services and about the fact you remain ultimately responsible for your work, even when using AI tools.</p> <p>rC20. You are personally responsible for your own conduct and your own professional work, including when using AI tools. You should be able to justify your decisions and actions, and you should be forthright about your use of AI when asked by a client or the court.</p> <p>CD9. You must be open and co-operative with your regulators, including by responding honestly and transparently to BSB enquiries about your use of AI, and by providing any information we may require about such use for the purposes of our regulatory functions (rC64).</p>

6. Your responsibilities when others use AI

*You should be aware **that clients, solicitors, and opposing parties might use AI tools to seek legal information, including publicly available tools that have limited reliability in legal contexts.***

Where you suspect clients are relying on AI in material they share with you, you are not required to engage in depth with the material, but you should consider whether the client understands its limitations and explain to the client the risks this use may pose, especially if you are instructed under direct access as they may not have other sources of advice or representation. You may also need to consider whether this use may compromise legal professional privilege or other rights and advise your client accordingly.

You should also be aware that instructing solicitors may use AI tools, and you should consider the impact this use may have on their instructions or the materials they provide. You may need to consider whether this use may impact the accuracy or confidentiality of materials they share with you.

Opposing litigants-in-person may also use AI tools to make legal arguments without fully understanding their implications, and you should also be aware of this possibility.

We encourage you to ensure that clients understand the nature of the service being provided, particularly when using AI tools in ways that could affect a client’s understanding of authorship, responsibility or reliability of information.

Where you are engaged to provide legal services, you remain responsible for the advice and work provided, even if AI tools are used to support the service. Clients should feel able to ask questions about how AI is used, what role it plays in the legal service, and who is accountable for the final advice.

<i>Why we’re interested:</i>	This expectation derives from Core Duty 2 (Best interests of each client), Core Duty 3 (Acting with Honesty and with Integrity), and Core Duty 5 (Trust and Confidence in you and in the profession)
<i>Key rules engaged</i>	rC123. If you are instructed directly by a lay client under the Public Access scheme, and you suspect the client is relying on information or advice from an AI system, you should consider whether the client understands the information they receive and whether it is accurate, in order to determine whether it may be in the best interests of that client or in the interest of justice for the client to instruct a solicitor or other professional client.