The ethics of AI: new PCRT guidance

General Features

May 2026



22 April 2026

PCRT’s new guidance highlights AI risks, requiring advisers to maintain oversight, transparency and responsibility through firm-wide policies and controls.

Key Points

What is the issue?
New PCRT guidance highlights how the use of AI creates ethical and professional risks, even though the underlying principles themselves have not changed.

What does it mean to me?
AI is now embedded across practice, so the PCRT standards apply more widely. Advisers remain responsible for the work produced and must ensure appropriate oversight, transparency and control.

What can I take away?
Firms should adopt a structured, firm-wide approach to AI, aligning engagement

terms, internal policies and day-to-day practice, and ensuring that all AI-assisted work is properly reviewed and supported.

The seven professional bodies that produce Professional Conduct in relation to Taxation (PCRT) issued updated guidance on 19 January 2026, including new material on the ethical use of artificial intelligence. While framed as an application of existing principles, the update reflects a significant shift in how professional work is carried out and how risk arises within that work.

AI is now embedded across research, analysis, communication and operational processes, often without a clear framework governing its use. The guidance does not change the underlying principles, but makes it clear that they apply fully in an AI-enabled environment. Failure to meet those standards may have professional and disciplinary consequences. This article considers what the guidance means in practice. It argues that firms should treat AI not as a technical issue, but as a firm-wide risk management matter requiring alignment of engagement terms, internal controls and day-to-day behaviour.

Why this matters beyond PCRT

PCRT sets the expected standard for members of seven professional bodies and is reflected in HMRC’s Standards for Agents. In practice, it is widely treated as the benchmark for professional conduct across the tax profession. Advisers who fall short may be exposed if their conduct is challenged, whether or not they are formally bound by it.

The new AI guidance should therefore be seen as part of the evolving baseline of professional conduct. It is likely to inform the expectations of regulators, insurers and courts.

Applying PCRT standards to tax work alone, while allowing a lower standard elsewhere, is unlikely to be sustainable. It risks creating confusion for staff, inconsistency for clients and increased exposure to claims or complaints.

The guidance is best understood as having firm-wide application. It is not simply about compliance, but about establishing a consistent and robust approach to the use of AI across the practice.

How AI is being used in practice

AI is already widely used within the tax sector. Its use generally falls into four broad categories, each with distinct risks.

1. Research

AI tools are increasingly used to summarise legislation, identify relevant authorities and provide initial responses to queries.

The benefit is speed and accessibility. The risk is that material generated may be incomplete, outdated or simply wrong, including references to legislation or case law that do not exist. Without verification, there is a real danger that such material is relied upon inappropriately.

2. Data processing and document review

AI is widely used to analyse data sets, review contracts or extract key information from reports or correspondence.

This can significantly improve efficiency, particularly in areas that would otherwise be labour intensive. However, the results produced depend on input quality and underlying assumptions. Errors at either stage can lead to flawed conclusions.

3. Note-taking and analysis

AI notetakers are increasingly used to record and summarise meetings, and to generate action points. While this can reduce administrative burden, it raises issues around accuracy, tone and confidentiality. Notes may mispresent discussions if they are not carefully reviewed.

4. Automation of processes

AI is used to automate workflows, reminders and aspects of client onboarding, including elements of anti-money laundering checks and data collection. Automation can improve consistency and efficiency, but creates risk if processes are not fully understood or if the work produced is not reviewed. Care must be taken to consider the potential for bias. There is a particular danger that automated outputs are

treated as inherently reliable.

Ethical principles in an AI context

The new guidance considers the use of AI through the lens of the core ethical principles underpinning PCRT. Their application in an AI context brings certain risks into sharper focus.

One of the most immediate concerns is the potential impact on integrity. There is a risk that AI-generated material may be accepted without sufficient scrutiny, particularly where it appears complete and authoritative.

Closely linked to this is the issue of transparency. Where AI plays a significant role, failure to recognise whether disclosure is appropriate may undermine trust.

Issues of professional competence and due care arise where AI outputs are relied upon without proper understanding or verification. AI responses may be persuasive but incorrect, incomplete or based on flawed assumptions. This results in a real risk that the quality of advice falls below the required standard. Despite the role of AI in the process, the duty of care remains firmly with the adviser.

Confidentiality presents further challenges, particularly when using publicly available tools. Firms must consider how client data is handled, stored and protected, and whether appropriate consent has been obtained.

There are also implications for professional behaviour. AI-generated communications may be inappropriate in tone or content if not carefully reviewed, potentially affecting relationships with clients, HMRC or other stakeholders. Careless or inappropriate use of AI has the potential to bring the profession into disrepute.

Recurring risks

Some themes arise repeatedly when considering how AI is used in practice. Transparency is a key issue. Clients may not be aware that AI is being used in the delivery of services. This is more problematic where it plays a material role in the service, particularly if the client would reasonably expect to be informed.

There is also a tendency towards over-reliance. AI-generated material often appears authoritative, even where it is incomplete or incorrect. Without careful review and verification, there is a real danger of uncritical acceptance, with consequences for the quality of advice provided.

Data handling presents further challenges. Inputting client information into AI tools, particularly publicly available ones, creates potential risks around confidentiality and data protection. These risks are not always immediately apparent.

Finally, AI is often adopted informally within firms without central oversight or clear guidance. This can lead to inconsistent practices and an increased exposure to both regulatory and professional risk.

Taken together, these issues highlight the need for a structured and deliberate approach to the use of AI, rather than reliance on ad hoc or uncoordinated practices.

AI and engagement terms: are you covered?

Many of the risks arising from the use of AI can be addressed through clear engagement terms. However, standard wording alone is unlikely to be sufficient.

- Firms need to ensure that their terms reflect how AI is actually used in practice. The following questions provide a practical starting point.
- Have you clearly stated in your engagement terms that AI may be used, and explained this where it is fundamental to the service?
- Do you understand how AI is used across your services so that your wording is accurate?
- Are your terms clear about the extent to which you rely on information provided by the client?
- Do your terms cover AI notetakers and the review of notes?
- Have you considered where data from AI tools is stored and any data protection implications?
- What would you do if a client objected to the use of AI?
- Can you distinguish between client-facing and internal AI use?
- Do you require clients to disclose where information they provide has been generated using AI?
- Do you have processes to apply professional judgement where information appears inconsistent?

AI and client data: key risk questions

- Are you entering any identifiable client information into public AI tools?
- Do you understand where that data is stored, and who may access it?
- Is anonymisation genuinely effective or could the client still be identified from context?
- Do staff understand that deleting names or obvious identifiers may not be sufficient to protect client confidentiality?
- Does your use of AI comply with GDPR, particularly where there is cross-border transfer of data?
- Do your engagement terms and client communications adequately address how data may be used?
- Are there any confidentiality agreements or NDAs in place that restrict how information can be handled?
- Do internal AI tools create risks around access to confidential information?

Common AI risks in practice

Hallucinations and inaccurate material: AI tools can produce plausible but incorrect material, including references to legislation or case law that are inaccurate or do not exist. Sources should be checked independently using authoritative materials. Firms should also consider how these checks are recorded on file to demonstrate that appropriate verification has taken place.

Untrained or inappropriate use of AI tools: Using AI without sufficient understanding creates a clear risk to professional competence. Firms should assess training needs for each tool in use, deliver appropriate training, and retain evidence of completion to demonstrate that professional standards have been met.

Use in producing documents (e.g. tax returns): Where AI is used within automated workflows, it is important to understand how those workflows operate and where risks may arise. Inputs and results should be subject to human review before submission. Any functionality that allows documents to be submitted without review should be disabled. Testing and error logging can help to identify issues.

Client data entered into public AI tools without consent: The use of public AI tools raises risks around confidentiality and data protection. Firms should use approved non-public tools wherever possible. Where public tools are used, data should be anonymised so that clients cannot be identified. Firms should also understand where data is stored and ensure that its use complies with GDPR and internal policies.

Client data subject to NDAs or enhanced confidentiality: Additional care is required where information is subject to a non-disclosure agreement or similar restrictions. Firms should have appropriate internal processes in place to flag such restrictions and prevent inadvertent disclosure, for example through the use of alerts or information barriers.

AI-assisted client advice: AI-assisted work must comply with professional standards. Firms should ensure that staff understand the limitations of the tools they are using, and that work produced is tested against what would be expected if it were carried out without AI. All advice should be reviewed and signed off by an appropriately qualified individual.

AI-drafted correspondence: Correspondence generated with the assistance of AI must be reviewed to ensure factual accuracy, appropriate tone and compliance with professional obligations. Inappropriate wording can affect outcomes for clients and may risk breaching professional standards.

Policies, training and internal governance

Firms should implement a clear, practical AI policy. This should set out which tools may be used within the firm, the purposes for which they can be used, the type of information that may be input, and the checks that must be carried out on any AI-generated material. Importantly, the policy needs to be usable in day-to-day work.

Training is equally important. Staff need to understand how to use AI tools properly. This includes knowing how to frame questions in a way that produces useful material, how to identify potential inaccuracies or inconsistencies, and when further verification is required. Training should be documented and kept up to date.

Monitoring is essential. File reviews should be adapted to consider how AI has been used and whether the work produced has been appropriately verified.

A further practical challenge is the risk of unauthorised or undisclosed use of AI by staff. In many firms, AI tools are already being used informally, sometimes without the knowledge of those responsible for risk management. Firms need to restrict the use of AI to approved tools and to make clear that undisclosed use is unacceptable.

Choosing and controlling AI tools

AI systems should not be adopted on an ad hoc basis. Firms need to understand, at a high level, how tools operate, what data they use, where that data is processed and stored, and its key limitations. This does not require deep technical expertise, but decisions should be conscious and documented.

Use of AI within the firm should generally be restricted to approved tools rather than left to individual choice, and significant updates should be treated in the same way as the introduction of a new tool.

The key risk, however, lies not in the tool itself but in the material it produces. AI-generated material can be persuasive but flawed, and the key safeguard is review. Such material should be approached with appropriate scepticism, tested against expected outcomes and, where necessary, verified by reference to original sources. A useful working assumption is to treat AI as a junior member of the team: helpful, but requiring supervision and challenge.

Firms should also consider how their use of AI is recorded on file, including the steps taken to check and verify responses. This may include retaining relevant prompts and responses, together with a record of verification.

Particular care is required where AI is used to analyse data or generate reports, as errors may arise from misunderstood inputs or inappropriate assumptions. Similar issues can arise where tools are applied across different clients or types of work without considering whether embedded assumptions remain appropriate. Automation can also create a false sense of reliability if work generated is not subject to proper review.

Conclusion

The inclusion of AI within PCRT is a clear recognition of how fundamentally these tools are reshaping professional practice. The ethical principles themselves have not changed, but the environment in which they are applied has. AI introduces new risks, often subtle and not immediately visible, that require a more deliberate and structured response than many firms currently have in place.

What the guidance makes clear is that responsibility has not shifted. The use of AI does not dilute the adviser's duty of care, nor does it provide a defence where things go wrong. If anything, it raises expectations. Work must still be carried out with appropriate skill, care and judgement, and the presence of AI in the process makes oversight and critical assessment more important, not less.

AI is a powerful and increasingly indispensable tool. But it is not a substitute for professional judgement, and it does not reduce responsibility. The adviser remains accountable for the outcome. The challenge is to ensure that, as the tools evolve, the standards applied to their use remain just as robust.

'Topical guidance covering the application of PCRT to the ethical use of artificial intelligence tools' can be found at tinyurl.com/2xc52dzp. Further information can be found at www.kareneckstein.co.uk/riskbites

© Getty images