Emerging technology: reshaping client confidentiality

General Features

October 2026

23 September 2026

Emerging technologies are creating new confidentiality risks, requiring tax firms to update policies, strengthen controls and guide staff on appropriate use.

Key Points

What is the issue?
Emerging technologies, from generative AI to smart glasses, are creating new ways for confidential client information to be captured, processed or shared, often before firms' policies and working practices have adapted.

What does it mean to me?
Tax advisers need to consider whether existing confidentiality, data protection and acceptable-use policies adequately cover AI tools, wearable devices and other technologies that staff may use informally in everyday work.

What can I take away?
Firms should focus on the underlying risk rather than individual technologies, with clear rules on recording and AI use, appropriate staff training, named responsibility for oversight and regular policy reviews.

Over recent months, a wave of well-known UK hospitality and leisure businesses has moved to restrict the use of Meta’s smart glasses. Wetherspoons has barred customers from using them to record staff or other patrons without consent, while ATG Theatres will ask audiences to remove them during performances.

Their response reflects a wider concern: emerging technologies are creating new confidentiality and information security risks faster than many organisations’ policies can keep pace. For tax and accountancy firms, entrusted with sensitive personal, financial and commercial information, the implications are potentially much more significant.

If businesses controlling a restaurant, theatre or event for a few hours consider the risk of covert recording serious enough to act, what should professional firms holding highly sensitive personal and commercial information for years at a time be doing?

Many firms may have given relatively little formal thought to the confidentiality risks created by emerging consumer technologies, from wearable recording devices to publicly available AI tools. The technology may be new, but the obligation to protect client confidentiality is not. Firms therefore need to understand where the risks arise, the potential legal and professional consequences, and whether their existing policies are still fit for purpose.

The changing risk landscape

Professional firms have always needed to protect sensitive information. Client files can contain financial records, personal data and commercially sensitive correspondence, with significant commercial, legal and reputational consequences if that information is compromised.

What has changed is the ease with which information can now be captured, processed and shared. Cyber security remains an obvious concern, but firms must

increasingly consider technologies that staff may use routinely, and with no intention of causing harm.

The wider information security risk is already substantial. The government's 'Cyber Security Breaches Survey 2025/26' found that 43% of UK businesses had identified a cyber security breach or attack in the previous 12 months, which the report estimates is equivalent to approximately 612,000 businesses. Among professional, scientific and technical businesses, the proportion rose to 54%.

Generative AI is perhaps the clearest example of how the risk is evolving. In January 2026, the seven professional bodies that jointly prepare Professional Conduct in Relation to Taxation (PCRT), including CIOT and ATT, issued guidance on the use of AI in tax work. It warns that inputting client data into publicly available AI tools is likely to breach client confidentiality unless the client has specifically consented to its use.

The risk arises precisely because these tools can become part of everyday working practices. A member of staff might use an AI assistant to produce a template, work from a precedent or summarise information from a client file, without appreciating the confidentiality implications of entering that information into an external system.

The potential consequences were highlighted by the Upper Tribunal in *Munir v Secretary of State for the Home Department* [2026] UKUT 81 (IAC). The tribunal observed that uploading confidential documents to an open-source AI tool could place that information in the public domain, breaching client confidentiality and waiving legal privilege. It added that such conduct could warrant referral to the relevant regulator and the Information Commissioner's Office.

Although the observation was not a finding against the professional concerned, the wider warning is relevant to regulated firms. Technologies that staff can access and use informally may create risks that existing confidentiality policies were never designed to address.

Smart glasses: a wider problem

Unlike a phone or handheld camera, smart glasses are designed to look much like ordinary eyewear, making it less obvious to those around the wearer that recording could be taking place.

Meta’s smart glasses have sold in the millions since launch and retail for under £400, pointing to their emergence as mainstream consumer technology rather than a passing novelty. The challenge for firms is that technologies can become commonplace long before organisations have decided how they should be used around confidential information.

For professional firms, the broader challenge is not simply whether to ban one type of device, but how to control the use of technologies capable of recording or transmitting confidential information in sensitive settings.

The European Data Protection Board has been examining the privacy risks and safeguards associated with smart glasses. There has been no corresponding change in UK law specifically addressing the devices, but firms do not need to wait for technology-specific legislation before considering whether their existing confidentiality and acceptable-use policies adequately address devices capable of discreetly capturing information.

Where the legal exposure sits

The legal exposure is not confined to one area. Depending on the circumstances, firms may face confidentiality and data protection obligations, employment and disciplinary questions and, in some cases, concerns about legal professional privilege.

UK GDPR requires personal data to be processed lawfully, fairly and transparently. Its transparency requirements include informing individuals about the collection and use of their personal data, which can include their image and voice. Covertly recording a client meeting, a colleague or confidential material on screen could therefore raise data protection concerns, alongside questions about the firm’s supervision, training and internal controls.

The difficulty is that employment contracts, staff handbooks and bring your own device (BYOD) policies were largely drafted with laptops and mobile phones in mind. They may say little about wearable devices, publicly available AI tools or other consumer technologies capable of capturing, processing or transmitting confidential information.

Firms therefore face not only the consequences of a confidentiality or data protection breach, but scrutiny of whether their policies, training and supervision were adequate to prevent it.

Consider a routine client meeting. A member of staff attends wearing smart glasses, perhaps for their note-taking or translation features rather than with any intention to record. Partway through a discussion of sensitive financial information, the client notices the device and asks whether the conversation has been recorded.

In that moment, the issue is not simply whether a rule has been broken, but whether the client still feels able to speak freely. The client may now doubt the confidentiality of that conversation, and potentially others involving the same member of staff. A complaint or request for information about what data was captured and how it was processed can leave the firm in the difficult position of having to prove a negative: that no recording took place.

If the firm has no policy on wearable technology, no record of having briefed staff and no clear procedure for responding to such a concern, providing that reassurance becomes much harder. Even where no recording occurred, the resulting uncertainty can damage client confidence and require considerable management time to investigate and resolve.

That illustrates the practical value of establishing the rules before an incident occurs. A firm that can point to a clear policy requiring recording-capable devices to be removed, declared or disabled in client meetings, supported by appropriate staff training, is in a much stronger position to demonstrate how confidential information is protected.

What firms should do now

The answer is unlikely to be a blanket ban on smart glasses or any other single category of device. Technology will continue to evolve, so firms need policies that address the underlying risks of capturing, processing and sharing confidential information rather than individual products.

As a starting point, firms should review their bring your own device (BYOD) and acceptable-use policies to ensure that they cover wearable devices, AI tools and other recording or data-processing technologies. Employment contracts and staff

handbooks should also make clear what recording is permitted on firm premises and in client meetings, and when recording-capable or AI-enabled devices must be declared or disabled.

Generative AI requires particular attention. Firms should identify which tools are approved, what uses are prohibited, whether and when client information can be entered, and where staff should seek guidance if they are unsure.

Firms should also consider how new technologies are assessed before they become embedded through informal use. Responsibility for this should sit with a named individual or group, rather than falling somewhere between IT, HR and compliance. Policies should then be reviewed regularly to ensure that they continue to reflect both technological developments and working practices.

Ultimately, the aim is not to anticipate every new device or application. It is to establish principles that enable staff to recognise when a new technology could put confidential information at risk, and to know what to do about it.

In conclusion

Smart glasses are unlikely to be the last consumer technology to create unexpected risks for professional firms. The wider lesson is that protecting client confidentiality now requires firms to think beyond conventional cyber threats and consider how everyday technologies are used in the workplace.

Technology will continue to change. The challenge for firms is to ensure that their policies, training and working practices change with it.