Helpsheet: The use of AI and technology in practice

Issued: August 2026
Last issued: August 2026
Last reviewed: August 2026

Introduction

This helpsheet is intended to support members and firms when using artificial intelligence (AI), automation, data analytics, cloud-based systems and other technology in practice. It isn't limited to the point at which a new tool is introduced. The principles should be applied before deployment, during use, when systems are changed, and as part of ongoing monitoring and review.

Technology can aid effectiveness through supporting efficiency, consistency and service quality, but it doesn't alter the professional responsibilities of members. Members remain responsible for the work they perform, approve or issue, including where technology has been used to support research, drafting, analysis, client communication, decision-making or administration.

Scope and application

This helpsheet applies to the use of AI and other technology in all aspects of practice, including client work, internal processes, quality control, compliance, training, marketing, knowledge management and practice administration.

Members should apply the principles set out in this helpsheet proportionately, taking account of the nature of the tool, the sensitivity of the information involved, the purpose for which it is used, the level of human oversight, and the potential impact on clients, staff, regulators and other stakeholders.

By necessity, this helpsheet is high-level and principles-based. It can't directly address every AI tool, software product or service that firms may use. Each product will have its own specific contractual terms, data flows, security features, configuration settings and risk profile. Firms should consider the particular tool and use case carefully and should seek advice from their managed IT service provider, software supplier, specialist consultant, data protection adviser or legal adviser if they're unsure about the appropriate approach.

Core principle: professional responsibility remains with the member

The use of AI or technology doesn't transfer responsibility from the member or firm to the technology provider. Members should be able to explain and justify the work they issue, the judgements they make, and the advice they provide, including where technological tools have contributed to the output.

Members should ensure that technology is used to support, not replace, professional judgement. AI-generated or technology-assisted outputs should be reviewed with an appropriate level of professional scepticism before they are relied upon, shared or incorporated into end service outputs.

Ethical considerations

The fundamental ethical principles still apply when using AI and other technology. Members should consider, on an ongoing basis, whether the use of a tool supports or threatens compliance with integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

Members may also find it useful to refer to the CCAB Draft Statement to the Accountancy Profession on the Ethical Use of Artificial Intelligence. The statement explains how the existing ethical framework applies to the development, procurement, deployment and use of AI tools and systems. It also reinforces that professional accountants remain responsible and accountable for work produced with the assistance of AI, and that this responsibility can't be delegated to technology.

- **Integrity:** Do not use technology in a way that could produce or present misleading information.
- **Objectivity:** Remain alert to bias, automation bias and over-reliance on system outputs.
- **Professional competence and due care:** Use tools only where users have sufficient understanding of their purpose, limitations and risks.
- **Confidentiality:** Protect client and firm information when selecting, configuring and using technology.
- **Professional behaviour:** Ensure that technology use is consistent with professional standards, legal obligations and public expectations.

Why AI and emerging technologies require particular attention

AI and other emerging technologies may have characteristics that make ethical and practical risks harder to identify and manage. These can include:

- **Opacity**, where it isn't clear how an output was generated.
- **Non-determinism**, where similar prompts may produce different results.
- **Data dependence**, where outputs are shaped by the quality and completeness of input data.
- **Adaptivity**, where systems or models change over time.
- **Autonomy**, which allows systems to make decisions or perform tasks with limited intervention or oversight from humans.
- **Scalability**, where the ability to maintain or improve performance when handling larger volumes of data or increased workloads, potentially magnifies both benefits and any existing biases or errors.
- **Speed**, where the ability to process information, complete tasks, or generate outputs rapidly, can increase the impact of both positive outcomes and mistakes, and may outpace effective human review or oversight.

These characteristics increase the importance of governance, professional scepticism, human review and clear accountability.

Governance across the technology lifecycle

Governance should not be treated as a one-off exercise at implementation. Firms should establish and maintain arrangements that apply throughout the lifecycle of AI or technology use. These arrangements should be proportionate to the risks presented by the tool and the context in which it is used.

Appropriate governance may include documented policies, approval processes, user guidance, training, review procedures, incident reporting, periodic reassessment and clear allocation of responsibility for oversight. Firms should also identify who AI-related issues should be reported to, such as the engagement partner, compliance lead, IT contact or another appropriate person, and make clear that concerns should be reported immediately.

For AI-enabled tools, governance should also cover the design and use of prompts and the quality of input data. Poorly framed prompts, incomplete information or biased data can affect the reliability, fairness and usefulness of outputs. Firms should consider whether users need guidance on how to structure prompts, what information should or shouldn't be included, how assumptions should be stated, and when outputs need additional review because the underlying data may be incomplete, unbalanced or not representative.

Lifecycle considerations

Firms should think about AI and technology use as an ongoing lifecycle rather than a one-off decision. The level of work needed at each stage will depend on the risk of the tool and how it is used, but each stage should prompt a proportionate check that the tool remains suitable, controlled and consistent with the firm's professional, ethical and legal obligations.

- **Selection:** Consider the purpose of the tool, the data it will use, the provider's credentials and whether the tool is suitable for the intended practice context.
- **Configuration:** Set appropriate access rights, data controls, retention settings and restrictions on use.
- **Use:** Ensure users understand permitted uses, review requirements and escalation routes.
- **Monitoring:** Review whether outputs remain reliable, appropriate and consistent with professional obligations.
- **Change:** Reassess risks when the tool, provider terms, data flows, functionality (including new or amended models) or intended use changes.
- **Exit:** Consider data retention, deletion, transfer and continuity arrangements when discontinuing a tool.

Examples of good governance

Good governance will vary depending on the size and complexity of the firm and the risks associated with the tool. However, examples of good governance may include the following:

- **Maintaining an approved tools register:** Keeping a current record of AI and technology tools used by the firm, including their purpose, owner, data inputs, approval status, review date and any restrictions on use.
- **Assigning clear ownership:** Allocating responsibility for each tool to a named role or team, including responsibility for oversight, risk assessment, user guidance and periodic review.This includes consideration of model or version updates being approved for use.
- **Documenting permitted and prohibited uses:** Providing staff with clear guidance on what tools may or may be used, what information may be entered, what outputs may be relied upon and when escalation is required.
- **Building in human review:** Requiring appropriately competent review before AI-assisted outputs are used in client advice, regulatory submissions (including the likes of tax returns or accounts), financial analysis, audit evidence or other higher-risk work (including provision of information to funders or other third parties) .
- **Managing prompts and input data:** Providing practical guidance on prompt design, avoiding unnecessary or sensitive data in prompts, recording important assumptions, and considering whether input data may be incomplete, outdated, skewed or otherwise biased.
- **Recording key decisions:** Retaining evidence of risk assessments, Data Protection Impact Assessments (DPIAs), supplier due diligence, approval decisions, review outcomes and changes to the tool or its use.
- **Monitoring actual use:** Periodically checking whether tools are being used as intended, whether staff understand the controls, and whether any unauthorised or informal use has emerged.
- **Refreshing controls when circumstances change:** Reassessing the tool when provider terms change, functionality is updated, new data is introduced, use cases expand, or legal, regulatory or professional expectations develop.

Confidentiality, data protection and information security

Members and firms should understand what information (including data) is entered, processed by, stored in or generated through a technology tool. Care should be taken where client confidential information, personal data, special category data, commercially sensitive information or regulatory information is involved.

Before and during use, firms should consider whether existing engagement terms, privacy notices, client communications, information security policies and data processing arrangements remain appropriate. This should be revisited when the nature of the processing, the tool's functionality or the provider's terms change.

Where personal data is processed, firms should consider whether a DPIA is required or advisable (see section UK General Data Protection Regulation (GDPR) considerations and compliance).

Example: Using client data beyond service delivery for that client

Firms should be careful before using client information for purposes beyond delivering the agreed services to that client. For example, a firm may want to use information from client accounts to create cross-client dashboards, benchmarking reports or sectoral insights, either for internal planning or to produce client briefings.

Before doing this, the firm should consider whether the proposed use is covered by the engagement letter, terms and conditions, privacy notice and any other client communications. If the original basis for receiving the information was to prepare accounts, tax returns, audit work or another specific service, it shouldn't be assumed that the same information can automatically be reused for wider purposes.

Where the firm wants to use client data for broader purposes, it must ensure that the data can be anonymised or aggregated so that clients and individuals can't be identified to meet the confidentiality principle within the ICAS Code of ethics. The firm should also consider whether the use is fair, transparent and compatible with the original purpose, whether a separate lawful basis is needed, whether client consent or updated engagement terms are required.

A practical approach is to decide this before the data is used: record the purpose, identify the data involved, check the client contract and privacy notice, decide whether anonymisation is sufficient, and update client-facing terms or communications if the firm wants to reserve the right to use information for benchmarking, dashboards or sector insights in future.

UK GDPR considerations and compliance

Where AI or other technology involves the processing of personal data, members and firms must consider their obligations under the UK GDPR and the Data Protection Act 2018. The Information Commissioner's Office (ICO) guidance on AI and data protection emphasises that organisations should apply data protection principles throughout the AI lifecycle, including accountability, lawfulness, fairness, transparency, data minimisation, security and ongoing governance.

Firms should identify the role they play in relation to each processing activity. In virtually all circumstances the firm will be a controller. The technology provider is most likely to be a data processor, or on occasions, be a joint data controller. These roles should be understood and documented, as they affect contractual requirements, accountability and responsibility for responding to data subject rights.

ICO guidance on AI

Firms using AI tools that process personal data should refer to the ICO's AI guidance, which brings together detailed guidance on AI and data protection, explaining decisions made with AI, and practical resources for assessing AI-related data protection risks.

Access the ICO AI guidance

Data Processor Agreements and supplier contracts

Where an AI or technology provider processes personal data on the firm's behalf, the firm should treat the Data Processor Agreement (DPA), or equivalent data processing terms, as a critical part of its UK GDPR compliance. As noted above, in many common software and cloud-service arrangements the firm will be the controller and the supplier will be the processor, although firms should still check the supplier's terms because some services or features may involve a different role.

A firm shouldn't use a tool to process personal data unless there is a written contract or other legally binding arrangement that meets UK GDPR processor requirements. This may be a standalone DPA, an addendum to the supplier's terms, or data processing clauses incorporated into the software terms and conditions. The firm should keep a copy or record of the terms relied on, including the version or date reviewed.

At a minimum, the DPA or data processing terms should set out the subject matter and duration of the processing, the nature and purpose of the processing, the types of personal data involved, the categories of data subjects, and the firm's rights and obligations. They should also require the processor to act only on the firm's documented instructions, maintain confidentiality, apply appropriate security measures, control the use of sub-processors, assist with data subject rights, support breach notification and DPIAs, deal properly with deletion or return of data at the end of the service, and provide information needed to demonstrate compliance.

For most firms, this doesn't usually mean negotiating bespoke terms with major software suppliers. A proportionate approach may be to review the supplier's standard DPA or data processing addendum, check that it addresses the key UK GDPR points, record any important limitations or configuration choices, and seek advice if the terms are unclear or the proposed use is higher risk.

Particular care should be taken with AI-specific processing terms. Firms should check whether prompts, uploaded documents, outputs or usage data are retained, reviewed by the supplier, used to improve or train models, transferred outside the UK, or shared with sub-processors. If the answer isn't clear, the firm should ask the supplier before using the tool with client or personal data.

Lawful basis of processing

Members and firms should be able to identify and document the lawful basis for each relevant processing activity. This may differ depending on whether the tool is being used for client service delivery, internal administration, quality control, training, analytics, fraud prevention, knowledge management or another purpose. Where special category data or criminal offence data is involved, additional conditions and safeguards will be required.

The lawful basis for the firm's processing doesn't remove the need for suitable processor terms where a supplier processes personal data on the firm's behalf. Firms should therefore consider lawful basis and processor contract requirements together: the lawful basis explains why the firm may process the data, while the DPA helps govern how the supplier may process it for the firm.

Transparency is a key compliance requirement. Firms should consider whether privacy notices, engagement terms and client communications adequately explain how personal data may be used in connection with AI or other technology. Explanations should be clear enough for individuals to understand the nature, purpose and potential consequences of the processing, particularly where technology supports decisions or recommendations that may affect them.

Other considerations

A DPIA should be carried out where processing is likely to result in a high risk to individuals. The ICO also describes DPIAs as good practice for major projects involving personal data. In the context of AI or technology deployment, a DPIA should describe the nature, scope, context and purposes of the processing; assess necessity and proportionality; identify risks to individuals; and record measures to mitigate those risks. An example DPIA for an accounting practice using approved AI tools such as Microsoft 365 Copilot and similar AI-assisted drafting, summarisation or research tools is available (See specimen document section below).

Firms should also consider data minimisation and retention. Personal data should not be entered into or retained within a tool unless this is necessary for a defined purpose. Where possible, firms should use anonymisation, pseudonymisation, redaction, access restrictions and retention controls to reduce risk.

Where a tool produces or supports decisions about individuals, firms should assess whether automated decision-making rules apply and whether appropriate safeguards are required. This may include providing meaningful information about the decision, enabling genuine human intervention, allowing individuals to make representations, and allowing them to contest a decision where required.

Firms should ensure that they can respond effectively to data subject rights requests. This includes understanding where personal data is held, how it is retrieved, whether it has been used to generate outputs or inferences, and how correction, restriction, objection, portability or deletion requests will be handled in practice.

International transfers should also be considered. If personal data is processed, accessed or stored outside the UK, firms should ensure that appropriate transfer mechanisms, contractual protections and due diligence arrangements are in place. Further information on international transfers is available on the ICO website.

Review, validation and quality control

Firms should define when and how technology-assisted outputs must be reviewed. The level of review should reflect the risk and significance of the output. Higher-risk uses, such as client advice, regulatory submissions, audit evidence, financial analysis or legal interpretation, should be subject to more robust review.

Review procedures should consider accuracy, completeness, relevance, bias, consistency with source materials, and whether conclusions are properly supported. Members should not rely on AI-generated content without checking it against appropriate professional knowledge, evidence and source material.

Members should remain alert to automation bias: the tendency to place undue reliance on technology-generated outputs because they have been produced by a system. Outputs should be assessed on their merits and challenged where appropriate, particularly where they appear authoritative, precise or confident but aren't clearly supported by the underlying evidence.

Review should also include a wider reasonableness check. Even where detailed checks have been completed, members should stand back and consider whether the output makes sense in the round: does it align with the client's circumstances, the known facts, the wider evidence base, professional experience and common sense? If the output appears technically correct but doesn't "stack up" when viewed against the bigger picture, it should be challenged, revised or escalated before it is relied on.

Members should also be alert to the possibility that documents, images, audio, video, messages or other information obtained from third parties may have been artificially generated or manipulated. Where the authenticity of material is important to the work being performed, firms should consider what checks are needed before relying on it.

Where review identifies a significant error, unexpected output, possible confidentiality issue, evidence of bias, inappropriate use of data, or a concern that the tool has been used outside approved parameters, this should be reported immediately to the appropriate person within the firm. The reviewer should consider whether the output should be withdrawn, corrected, subject to further review, or logged as an incident.

Transparency and client communication

Firms should consider whether, and how, clients should be informed about the use of AI or technology. This will depend on the nature of the tool, the type of data processed, contractual arrangements, regulatory expectations and whether the technology materially affects how services are delivered.

There may not always be a need for separate client consent solely because a tool is used internally. However, transparency may be required or appropriate where client data is processed in a materially different way, sensitive information is involved, automated decision-making is used, or client expectations would reasonably require disclosure.

Training and user awareness

Users should receive appropriate training on the tools they are permitted to use. Training should cover permitted and prohibited tools and uses, confidentiality, data protection, prompt quality, output review, escalation routes, immediate incident reporting and the limitations of the tool.

Firms should also make clear that informal or unsanctioned use of publicly available tools may create risks. The use of unapproved applications, services or AI tools, sometimes referred to as “shadow IT”, may circumvent firm controls and increase confidentiality, security and compliance risks. Staff should know which tools are approved for use and, where appropriate, how to check it is an approved tool that is being used, what information may be entered into them, and when advice or approval should be sought.

Incident reporting and ongoing review

Firms should have procedures for immediately reporting and responding to concerns arising from the use of AI or technology. Concerns may be identified for example during review of technology-assisted outputs (see section above on Review, validation and quality) or governance processes. Users should know who to contact within the firm and should be encouraged to report issues as soon as they are identified, rather than waiting for a periodic review. This may include inaccurate outputs, inappropriate disclosure of information, unexpected system behaviour, security concerns, bias, use outside approved parameters, or any situation where a user is unsure whether the tool has been used appropriately.

Technology use should be reviewed periodically. Reviews should consider whether the tool remains suitable, whether controls remain effective, whether staff are using the tool appropriately, and whether changes in law, regulation, professional standards or provider terms require updates to the firm’s approach.

Practical checklist

This checklist is intended as a practical prompt for members and firms when considering whether their use of AI or technology is appropriately controlled. It can be used when assessing a new tool, reviewing an existing tool, preparing for an internal discussion, or recording the basis for a proportionate decision.

- Is the purpose of the tool clearly understood?
- Is the use of the tool consistent with professional, ethical and legal obligations? Is there any adverse media that might require to be factored into considerations?
- What data is entered, processed, stored or generated?
- Are client confidentiality and data protection obligations addressed?
- Are engagement letters, privacy notices and internal policies still appropriate?
- Has the firm identified the relevant UK GDPR role, lawful basis and any additional conditions for special category or criminal offence data?
- Are privacy notices, engagement terms and client communications sufficiently transparent about relevant processing?
- Can the firm respond effectively to data subject rights requests involving data held in or generated through the tool?
- Have international transfers, processor arrangements and contractual protections been assessed?
- Is there a suitable DPA or equivalent data processing terms for each supplier that processes personal data on the firm’s behalf?
- Do the processor terms cover documented instructions, confidentiality, security, sub-processors, data subject rights, breach support, DPIA support, audit or compliance information, and deletion or return of data?
- Are users trained and clear on permitted use?
- Are outputs reviewed by appropriately competent individuals?
- Has the reviewer stood back and considered whether the output makes sense in the round, taking account of the known facts, wider context, professional knowledge and experience?
- Are risks such as bias, hallucination, automation bias and lack of explainability considered?
- Are incidents, errors and concerns reported immediately to an appropriate person within the firm and addressed promptly?
- Is the tool and models subject to periodic review and reassessment?
- Is there a plan for changing, replacing or discontinuing the tool?

Frequently asked questions

Can a firm use AI tools in client work?

Yes, provided the firm has considered whether the tool is appropriate for the task, whether client confidentiality and data protection obligations are met, and whether outputs are reviewed by someone with suitable knowledge and experience before they are relied on or shared.

Does using AI change who is responsible for the work?

No. Responsibility remains with the member or firm. AI can support research, drafting, summarisation or analysis, but it doesn't replace professional judgement, professional scepticism or normal quality control.

Can client data be entered into AI tools?

Only where the firm is satisfied that this is permitted, necessary and appropriately controlled. Firms should use approved tools, avoid public or unapproved tools for client data, check supplier terms and settings, and minimise or anonymise data where possible.

Is separate client consent always required before using AI?

Not necessarily. It will depend on the nature of the tool, the data involved, the purpose of the processing, the engagement terms, the privacy notice and client expectations. Updated terms, privacy notices or specific consent may be needed where client data is used in a materially different way.

Do firms need to carry out a DPIA for every AI tool?

No. A DPIA is required where processing is likely to result in a high risk to individuals, and it may be good practice for significant projects involving personal data. Firms should take a proportionate approach and record why a DPIA is or isn't needed.

What should firms check with software suppliers?

Firms should ask for clear information about how UK GDPR compliance is supported by the product. They should check what data is processed, where it is stored, whether sub-processors are used, whether data is used for AI model training, what security measures apply, and which configuration settings should be reviewed before use. They should also ensure that suitable Data Processor Agreement clauses are included in the software terms and conditions, or that a separate Data Processor Agreement is in place, before personal data is processed through the tool.

Can AI outputs be used in client advice or deliverables?

They can be used to support drafting or analysis, but they should not be treated as final without appropriate review. The reviewer should check accuracy, completeness, assumptions, source material, references and whether the output is suitable for the client's circumstances. Irrespective of detailed review, output should also be assessed in the round for overall reasonableness based on knowledge, experience and professional judgement. If output appears technically incorrect or doesn't stack up against the bigger picture it should be challenged, revised or escalated before being relied on or shared.

What should staff do if something goes wrong?

They should report the issue immediately to the appropriate person within the firm. This may include inaccurate outputs, unexpected results, confidentiality concerns, suspected bias, use outside approved parameters, hallucinations, or any uncertainty about whether the tool has been used appropriately.

Specimen Documents

Template approved tool register

Example Data Protection Impact Assessment (DPIA)

Useful links

GDPR helpsheets

Snapshot: Ethics and Independence Approach to the Use of Technology (International Ethics Standards Board for Accountants – June 2026)

Emerging Technologies: A Characteristics-Based Approach to Ethical Considerations for Professional Accountants (International Ethics Standards Board for Accountants July 2026)

Ethical use of AI (CA Mag – March 2026)

ICAS Code of Ethics:

- Fundamental principles (subsections 110 to 115);
- Section 120 - Conceptual Framework (this includes the inquiring mind, professional judgement, bias etc)
- Section 200.6 A2 – 200.7 A5 (Professional Accountants in Business (PAIB)) - Identifying Threats Associated with the Use of Technology
- R220.4 – Preparation of Information (PAIB)
- R220.8 – 220.8 A1 – Using the output of technology
- 220.12 A4 - Considering using the work of others or the output of technology
- 300.6 A2 - Identifying Threats Associated with the Use of Technology (Professional Accountant in Practice (PAPP)
- R320.11 – 320.12 A1 Using the output of technology (PAPP)

Further information and assistance

Further assistance and information can be obtained from the Practice Support team. You can contact them through the Practice Support section of the ICAS Technical helpdesk.