Artificial Intelligence and Client Data Processing Policy

How we use artificial intelligence in the delivery of our accounting and advisory services, and the safeguards we apply to client information.

Policy owner	COO
Approved by	COO
Version	1.1
Effective date	01 June 2026
Next review	31 May 2027
Applies to	All OCFO partners, directors, employees, contractors and third parties processing client information on our behalf, across our South African, United Kingdom and United States operations.
Classification	Public — published on our website and available to clients, prospective clients and insurers on request.

1. Purpose of this policy

OCFO uses carefully selected artificial intelligence (AI) tools to help us deliver accurate, timely and cost-effective accounting and advisory services. This policy sets out, openly and in plain language:

- why and how we use AI in the course of our work;
- the bases on which we process personal and confidential client information through these tools;
- the safeguards, controls and human oversight we apply to protect that information; and
- the standards we hold ourselves to, and how clients can raise questions or exercise their rights.

We publish this policy so that our clients, their data subjects and our professional indemnity insurers can clearly understand our approach to AI and the risk-management framework that sits behind it. We regard responsible AI governance as part of our professional duty of care, not as an optional extra.

2. Scope

This policy applies to all use of AI tools by OCFO and by any third party acting on our behalf, wherever that processing involves client information — including personal information, financial records, management information and other confidential business data.

It covers our South African operations (governed principally by the Protection of Personal Information Act, 2013 ("POPIA")), our United Kingdom operations (governed principally by the UK General Data Protection Regulation and the Data Protection Act 2018 (together, "UK data protection law")), and our United States operations.

The United States has no single federal data protection law equivalent to POPIA or UK data protection law. Instead, a combination of federal sector-specific rules and state privacy laws applies. Where relevant to our services, this includes US state comprehensive privacy laws (such as the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and the comparable laws now in effect in around twenty states) and federal rules governing financial and tax information. All US operations are bound by New York laws.

This policy sits alongside, and should be read with, our broader Privacy Policy. Where this policy refers to internal procedures, those procedures are maintained separately and are available to our regulators and insurers on request.

3. Key terms

Artificial intelligence (AI) tools — software systems, including generative AI and machine-learning models, that process inputs to produce outputs such as text, analysis, classifications, summaries or calculations.

Client information — any data relating to a client or a client's affairs that we hold or process, including personal information about identifiable individuals (for example employees, directors or customers of our clients).

Personal information / personal data — information relating to an identified or identifiable natural person, as defined under POPIA, UK data protection law and applicable US state privacy laws respectively.

Processing — any operation performed on information, including collection, storage, analysis, generation, use, sharing and deletion.

Human-in-the-loop — a control under which a member of our team reviews, validates and takes responsibility for AI-assisted output before it is relied upon or shared.

4. Our guiding principles

Our use of AI is governed by the following commitments, which align with the data-protection principles under POPIA, UK data protection law and applicable US privacy laws:

1. Human accountability. AI assists our professionals; it does not replace their judgement. A person remains responsible for every deliverable.
2. Lawfulness, fairness and transparency. We process client information through AI only where we are permitted to, and we are open about doing so.
3. Purpose limitation. We use AI only for the legitimate purposes of delivering and improving our services, not for unrelated purposes.
4. Data minimisation. We limit the personal information disclosed to AI tools to what is necessary for the task.
5. Accuracy. We verify AI-assisted output before relying on it, recognising that AI can produce confident but incorrect results.
6. Security and confidentiality. We use enterprise-grade tools with contractual protections and we maintain professional confidentiality at all times.
7. Accountability and review. We document our controls, assess risks and review this policy regularly.

5. How and why we use AI

We use AI tools to support tasks such, including but not limited to the following:

- drafting, summarising and reviewing documents, correspondence and reports;

- organising, categorising and reconciling financial data and transactions;
- extracting information from documents and source records;
- preparing first-draft analysis, calculations and management information for professional review;
- research on accounting, tax and regulatory matters;
- other connected APP platforms;

We do not use AI to make solely automated decisions that produce legal or similarly significant effects on individuals without meaningful human involvement. Where any element of automated decision-making is contemplated, we assess it separately under section 71 of POPIA, Article 22 of the UK GDPR, and applicable US state privacy law before proceeding.

6. How we process information lawfully

Where we process personal information through AI tools under POPIA or UK data protection law, we rely on one or more of the following lawful bases, identified on a case-by-case basis:

- Performance of our engagement — processing necessary to deliver the services set out in our engagement letter with the client;
- Legitimate interests — our legitimate interest, or that of our client, in delivering services efficiently and accurately, balanced against the rights of the individuals concerned;
- Legal obligation — processing required to meet our regulatory and statutory obligations; and
- Consent — where appropriate and obtained.

In most engagements, OCFO acts as a processor / operator / service provider of client personal information and the client is the controller / responsible party / business. Our use of AI to process that information is carried out under the client's documented instructions and the terms of our engagement. Where we determine the purpose and means of processing, we act as controller and apply this policy accordingly.

United States privacy laws generally operate on a notice-and-choice and consumer-rights model rather than the "lawful basis" concept used under POPIA and UK data protection law. For our US operations we provide the privacy notices required by applicable law and honour the consumer rights described in section 11.

7. Safeguards and controls

7.1 Human oversight

Every AI-assisted output is reviewed by a member of our team before it is relied upon, communicated to a client or used in a deliverable. The reviewing professional, not the tool, is accountable for the work.

7.2 Data minimisation and confidentiality

Where practical, we limit or remove identifying details. All client information processed through AI remains subject to our professional duty of confidentiality.

7.3 No use of client data to train public models

We use AI tools under business terms that contractually prevent our client inputs and outputs from being used to train the provider's public models. We do not enter confidential client information into consumer or free AI tools that do not offer these protections.

7.4 Accuracy and verification

We recognise that AI can generate plausible but incorrect or incomplete results. We therefore verify AI-assisted output against source records and our own professional judgement before relying on it. AI is a tool that supports our analysis; it is never the sole basis for professional advice.

7.5 Security

We protect client information processed through AI using appropriate technical and organisational measures, including access controls, encryption in transit and at rest, multi-factor authentication and supplier security assessments, consistent with our Information Security Policy.

8. AI providers and sub-processors

We carry out due diligence on the providers of the AI tools we use, and we put written contracts in place that include data-protection and confidentiality obligations. Our assessment considers, among other things:

- the provider's security and data-protection track record;
- whether client data is used for model training (and our right to opt out);
- data retention and deletion terms;
- the location of processing and any cross-border transfers; and
- the availability of appropriate contractual safeguards.

A current list of the principal AI tools and providers we use is available to clients and insurers on request.

9. Cross-border transfers

Because we operate in South Africa, the United Kingdom and the United States, and because some AI providers process data outside these jurisdictions, client information may be transferred across borders. Where this occurs, we apply the transfer safeguards required by the applicable law — for example POPIA (Chapter 9, section 72); UK data protection law (UK International Data Transfer Agreements, the UK Addendum to the EU Standard Contractual Clauses, or transfers to jurisdictions covered by UK adequacy regulations); and the contractual and disclosure requirements of applicable US state and federal law.

10. What we do not do

To protect our clients, we do not:

- use consumer or free AI tools for confidential client information;
- rely on AI output without human review;
- use AI to make solely automated decisions with legal or similarly significant effects on individuals without human involvement and an appropriate assessment;
- permit client data to be used to train public AI models; or
- use AI in any way that conflicts with our professional, ethical or regulatory obligations.

11. Your rights and how to contact us

Individuals whose personal information we process retain all rights available to them under the applicable law. Depending on where the individual is, these may include rights of access, correction, deletion and objection; under US state privacy laws, rights to access, correct and delete personal information, to opt out of its sale or sharing and of certain profiling; and the right not to be subject to certain solely automated decisions.

Because we often act as a processor (or, in US terms, a service provider) on behalf of a client, requests relating to a client's data subjects may need to be directed to, or coordinated with, that client. We will assist clients in responding to such requests. To raise a question about this policy or about our use of AI, or to exercise a right, please contact our information officer. You also have the right to complain to the relevant regulator: the Information Regulator (South Africa); the Information Commissioner's Office (United Kingdom); or, in the United States, the relevant state attorney general, the California Privacy Protection Agency or the Federal Trade Commission.

12. Governance and accountability

Responsibility for this policy and for our AI governance sits at board level. Our framework includes:

- Risk assessment — we carry out data protection impact assessments (DPIAs) and equivalent risk assessments for higher-risk AI processing before deployment, and keep them under review;
- Approved-tools register — only tools approved through our governance process may be used for client information;
- Training — our people receive guidance on the responsible use of AI and on this policy; and
- Monitoring and review — we review our AI use, controls and this policy at least annually and in response to regulatory or technological change.

13. Incidents and breaches

If a security compromise or personal-information breach involving an AI tool occurs, we follow our incident-response procedure, which includes containment, assessment, notification to affected clients and, where required, notification to the Information Regulator (within the timeframe required under POPIA), the Information Commissioner's Office (within 72 hours under UK data protection law), and the authorities and individuals required under applicable US state breach-notification laws.

14. Professional standards and risk management

OCFO maintains professional indemnity insurance appropriate to the services we provide. Our use of AI is conducted within our professional, ethical and regulatory obligations, and our risk-management framework — including the human-oversight and verification controls described above — is designed to manage the risks that AI can introduce, such as inaccurate output.

We disclose our use of AI to our professional indemnity insurers as part of the fair presentation of risk at placement and renewal, and we maintain the internal governance described in this policy to support that disclosure.

15. Review of this policy

We will review this policy at least annually and update it to reflect changes in our use of AI, in technology, or in the law — including forthcoming developments such as the UK's statutory Code of

Practice on AI and automated decision-making, South Africa's emerging national AI framework, and US developments such as California's automated decision-making technology rules and the evolving patchwork of state privacy and AI laws. The version and review dates are shown in the document-control table at the front of this document.

This policy is provided for transparency and does not form part of, or vary, any engagement letter or contract between OCFO and a client unless expressly incorporated by agreement.