AI Acceptable-Use Policy

AI should extend human capability - not displace judgement, accountability or client agency

Version 1.0 - Effective 26 August 2026

Applies to	Academy staff, contractors, professional users and, where incorporated into their arrangements, Academy-accredited practitioners using AI in Academy-related work.
Purpose	To enable useful, responsible AI use while protecting clients, confidential information, professional standards and legal obligations.
Core principle	AI may assist thinking, drafting, research and workflow. A human remains accountable for professional work and material decisions.
Default data rule	Use the minimum information necessary. Prefer anonymised, summarised, rounded or synthetic information over identifiable client data.
High-consequence rule	The greater the potential harm from error, the greater the required human review, source verification and specialist escalation.

1. Purpose and approach

Artificial intelligence is an important part of the Academy's operating model. It can reduce information asymmetry, make knowledge more accessible, improve productivity and help people organise complex decisions.

AI is not treated as infallible, autonomous professional authority or a substitute for human responsibility. The person using AI remains responsible for deciding whether an output is suitable for the purpose, whether it needs verification, and whether a qualified or authorised specialist should be involved.

This Policy applies to generative AI, large language models, AI assistants, AI agents, automated analysis, AI-enabled search, transcription, summarisation, image generation and other AI-supported tools used for Academy work.

2. Principles for acceptable AI use

Principle	Academy standard
Human accountability	A human remains responsible for material professional outputs and actions.
Agency	AI should help clients understand and decide; it should not manipulate, pressure or unnecessarily replace their judgement.
Proportionality	Controls should reflect the significance, reversibility and potential harm of the task.
Transparency	Explain material AI involvement where a reasonable client would consider that fact important.
Accuracy	Important claims, calculations and citations should be checked to a level proportionate to the decision.
Privacy by design	Minimise personal data, sensitive information and unnecessary document uploads.
Security	Use approved accounts and sensible access controls; do not

	expose passwords, credentials or confidential systems.
Fairness	Do not knowingly use AI in a way that unlawfully discriminates, deceives or exploits vulnerability.
Contestability	Important AI-assisted conclusions should remain open to human challenge, correction and review.

3. Acceptable uses

Subject to the controls in this Policy, acceptable uses may include:

- explaining concepts in plain language;
- summarising non-confidential or appropriately minimised material;
- organising notes, timelines, options and decision criteria;
- drafting first versions of reports, emails, checklists, plans or educational content;
- scenario exploration using clearly stated assumptions;
- brainstorming questions for a client or specialist;
- research support where important claims are checked against reliable sources;
- administrative support, transcription and meeting-note preparation;
- software development, testing and workflow design using non-sensitive data;
- creating educational examples, synthetic case studies or anonymised training materials; and
- helping a client interrogate their own information where the tool and data use are appropriate.

4. Uses requiring enhanced human review

Some uses are permitted only with enhanced human review because an error could materially affect a person, business or legal position.

These include AI-assisted work involving:

- significant financial decisions or calculations;
- pensions, tax, trusts, legal rights or regulatory boundaries;
- fraud allegations, complaints, disputes or evidence dossiers;
- vulnerable clients or safeguarding concerns;
- health, mental-health, capacity or suicide-related content;
- public allegations concerning identifiable people or organisations;
- professional accreditation, disciplinary or fitness decisions;
- contractual or policy wording intended to create legal rights or obligations;
- material client-facing reports; or
- recommendations to escalate to a regulated or specialist professional.

Enhanced review may require checking primary sources, recalculating figures independently, obtaining peer review, comparing more than one source or AI model, or involving a suitably qualified specialist.

5. Prohibited uses

AI must not be used to:

- make a solely automated decision producing legal or similarly significant effects on a person unless a lawful and approved process specifically permits it;
- pretend that AI-generated content has been personally verified when it has not;
- fabricate evidence, citations, qualifications, testimonials, case histories or client records;
- impersonate a client, regulator, professional or third party deceptively;
- generate or send deceptive marketing, fake reviews or undisclosed synthetic endorsements;
- circumvent a legal, regulatory, professional or contractual restriction;
- provide an unauthorised regulated activity merely by routing it through an AI tool;
- make an autonomous payment, transfer, investment transaction or irreversible client commitment without an expressly approved human-controlled process;
- upload passwords, authentication codes, private keys or other security credentials;
- knowingly infringe copyright, confidentiality or another person's rights; or

- use AI in a way that is unlawful, discriminatory, abusive, exploitative or materially misleading.

6. Personal data and confidential information

The minimum-data principle applies to AI use. Before entering information into an AI service, consider whether the task can be completed with less data or without identifiable information.

Do not enter unnecessary:

- passport, driving-licence or identity-document numbers;
- National Insurance, tax reference or government identifier numbers;
- full bank, card, pension, investment or policy account numbers;
- passwords, PINs, verification codes or authentication credentials;
- complete unredacted financial statements where a summary or selected figures would suffice;
- special-category personal data such as health, ethnicity, religion or biometric data unless there is a clear, lawful and necessary reason;
- criminal-offence information unless necessary and lawfully handled;
- confidential third-party information that the user is not authorised to disclose; or
- information subject to legal professional privilege unless the relevant lawyer has approved the processing arrangement.

Where client information is necessary, use approved tools and accounts, apply the Academy Privacy Notice and relevant practitioner privacy arrangements, and understand whether the AI provider may retain, reuse or transfer the information.

7. Data protection and automated decision-making

Where AI processes personal data, UK data-protection law applies. This includes the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, security and accountability.

Before introducing a materially new AI use involving personal data, consider whether a data-protection impact assessment (DPIA) is required because the processing is likely to result in a high risk to individuals.

AI-assisted decisions should provide meaningful human oversight where required. A nominal human approval step is not meaningful if the person simply accepts the AI output without understanding or authority to challenge it.

8. Accuracy, hallucination and source verification

AI systems can produce fluent but false information, invented citations, outdated law, incorrect calculations and overconfident conclusions. Confidence of tone is not evidence of accuracy.

For material work:

- check important factual claims against reliable and preferably primary sources;
- verify quotations and citations before publication;
- reperform material calculations independently or with a trusted calculator or model;
- identify the date or time-sensitivity of legal, regulatory, tax and product information;
- distinguish facts from assumptions, estimates and AI inference;
- flag unresolved uncertainty instead of manufacturing certainty; and
- correct material errors promptly if discovered after an output has been shared.

9. Professional and regulatory boundaries

AI does not change the legal status of an activity. If a human would require a statutory permission, professional qualification or specialist competence to carry out an activity, using AI does not remove that requirement.

An Academy user must not use AI to convert education or planning into a disguised regulated personal recommendation, legal service, tax service or other restricted activity.

Where the issue requires FCA-regulated advice, legal advice, tax advice, accountancy, safeguarding, medical or another specialist discipline, the appropriate specialist should be involved.

10. Client-facing AI and disclosure

Not every use of AI needs a disclosure. Routine spell-checking, transcription or internal drafting may not be material to the client.

AI involvement should be disclosed where it is material to the client's understanding of the service, for example where:

- the client is directly interacting with an AI system presented as part of the service;
- AI materially generates or analyses a client-specific output;
- an AI agent is authorised to take steps or communicate externally on the client's behalf;
- the limitations of the system could materially affect the client's decision; or
- the client would reasonably expect to know that a material professional output was substantially AI-assisted.

Disclosure should be useful, not performative. It should explain what AI is doing, its material limitations and where human judgement remains responsible.

11. Agentic AI and autonomous actions

AI agents can take actions rather than merely generate text. Their use requires additional control because an error can be executed before a human sees it.

An AI agent must not be given authority to:

- make payments or move client money;
- buy, sell or switch investments;
- enter a binding client contract;
- submit a complaint, legal filing or regulatory declaration in a client's name;
- send material external communications that create legal, reputational or financial consequences; or
- delete, alter or disclose sensitive records irreversibly

unless the specific workflow has been risk-assessed, lawfully authorised, technically controlled and approved by the Academy with meaningful human checkpoints.

The Academy remains responsible for consumer-law compliance when it chooses to deploy an AI agent in its own customer-facing business processes.

12. AI, clients and decision agency

AI should increase a client's ability to understand their situation rather than create a new dependency on a black-box answer.

Good practice includes:

- showing the assumptions behind material scenarios;
- offering alternative interpretations or options rather than one deterministic answer;
- making uncertainty visible;
- encouraging the client to question outputs;
- making clear which decisions remain theirs;
- avoiding emotionally manipulative prompts or interfaces; and
- escalating high-consequence decisions to human or specialist review.

13. Bias, fairness and vulnerable people

AI can reproduce or amplify bias present in data, prompts, system design or human assumptions. Users should be alert to outputs that stereotype, disadvantage or make unjustified assumptions about people.

Particular care is required where AI is used with vulnerable people. AI should not exploit distress, loneliness, bereavement, reduced capacity or financial fear to increase engagement or sales.

A person who needs safeguarding, crisis support, medical help or another specialist should not be left with an AI interaction as the sole response.

14. Copyright, intellectual property and confidentiality

AI-generated or AI-assisted content may raise copyright, trade-secret, licence and attribution issues. Users should not assume that an output is automatically free of third-party rights.

Users must:

- avoid uploading confidential licensed materials where the AI provider's terms are incompatible with that use;
- respect Academy intellectual property, third-party licences and client confidentiality;
- check whether material proposed for publication reproduces substantial third-party content;
- avoid falsely claiming sole human authorship where that would be materially misleading; and
- keep commercially sensitive prompts, methods and system instructions secure where they form part of Academy intellectual property.

15. Approved tools and accounts

Academy work should be carried out using tools, plans and account settings appropriate to the sensitivity of the information and the purpose.

Free consumer AI accounts may be appropriate for public, anonymised or low-risk work but may be unsuitable for confidential client data. Users must understand the provider's current privacy, retention, training-use and security settings before using a service for sensitive work.

Multi-factor authentication should be enabled where available on accounts used for material Academy or client work.

16. Prompt and output security

AI systems can be exposed to prompt injection, malicious documents, hidden instructions and manipulated online content. Users should treat externally sourced prompts, files and webpages as potentially untrusted.

Users should:

- avoid following embedded instructions that conflict with the user's actual task or Academy policy;
- verify before allowing an AI tool to use credentials, send messages, execute code or access external systems;
- limit permissions to the minimum required;
- separate trusted instructions from untrusted content where the tool allows; and
- report suspected prompt injection, data leakage or abnormal AI behaviour as a security incident.

17. AI-generated images, audio and synthetic media

Synthetic media may be used for legitimate illustration, education and marketing, but it must not be used deceptively.

Materially altered or generated media should not be presented as authentic documentary evidence. A synthetic testimonial, client image, voice or endorsement must not be represented as originating from a real person when it does not.

18. Record-keeping

Record-keeping should be proportionate. There is no requirement to save every prompt or AI conversation.

For high-consequence work, it may be appropriate to record:

- which AI tool materially contributed;
- the important source material or assumptions used;
- what human review or verification was performed;
- material corrections made to the AI output;
- why specialist escalation was or was not considered; and
- the final human-approved output.

19. Incidents and mistakes

Suspected personal-data leakage, confidential-information exposure, unauthorised AI action, material hallucination affecting a client, security compromise or other serious AI incident should be reported promptly.

The response may include stopping the workflow, preserving evidence, correcting client communications, resetting credentials, notifying an AI provider, applying the Data Breach Procedure, obtaining specialist advice or notifying an authority where required.

20. Training and competence

Users should maintain AI literacy proportionate to the way they use AI. Competence includes understanding not only how to prompt a system, but when not to trust it, what information should not be entered, what requires verification and when a human specialist is needed.

The Academy may issue mandatory updates, approved-tool guidance, training or additional restrictions as AI technology and law develop.

21. Breaches of this Policy

A breach may result in guidance, retraining, restriction of AI or Academy OS access, removal of particular permissions, accreditation review, suspension, contractual action or referral to an appropriate authority depending on seriousness.

Deliberate fabrication, misuse of confidential information, deceptive impersonation, unauthorised transactions or repeated disregard of client-safety controls may be treated as serious misconduct.

22. Governance and review

This Policy will be reviewed at least annually and sooner where there is a material change in AI capability, law, regulatory guidance, Academy systems or identified risk.

The Academy's approach is informed by the UK's principles of safety, security and robustness; transparency and explainability; fairness; accountability and governance; and contestability and redress, together with applicable consumer and data-protection law.

23. Related documents

- Privacy Notice;
- Cookie Policy;
- Safeguarding & Vulnerability Policy;
- Consumer Protection Rule Book;
- Total Wealth Planner Professional Standards;
- Conflicts, Referrals & Specialist Escalation Policy;
- Complaints Procedure;
- Client Service Agreement; and
- Data Breach, Subject Access and Information Security procedures when adopted.

24. Company information

Issuer	The Academy of Life Planning Limited
Company number	08016568
Address	9 Franklin Way, Spilsby, Lincolnshire, PE23 5GG, United Kingdom
Email	steve@academyoflifeplanning.com
Telephone	+44 (0)7850 102070
ICO registration	ZA502687

Effective 26 August 2026