

Artificial Intelligence (AI) Use Policy

VERSION 2.0

SEPTEMBER 2025





1. Purpose of this Policy

The purpose of this policy is to define how Artificial Intelligence (AI) is used within Rigour Research. It establishes safeguards, responsibilities, and governance to ensure AI is applied ethically, transparently and in a way that supports, rather than replaces, human decision-making. This policy also supports compliance with GDPR, ISO 27001, client contracts and industry best practice.

2. Scope

This policy applies to:

- All employees, contractors, and temporary staff
- All departments using AI-assisted tools or services
- Any AI used in relation to research activities, data collection, quality control, project delivery, internal processes or client work

It covers both internally developed tools and external AI platforms, whether on-premise, cloud-based, or embedded in third-party software.

3. Guiding Principles

Rigour Research's use of AI is governed by the following principles:

- **Augmentation, not replacement:** AI supports analysts and decision-makers. It never operates independently of human oversight.
- **Transparency:** AI use must be explainable and traceable. Staff must understand when and how AI outputs are produced.
- **Accountability:** Final responsibility for outputs, decisions or actions always rests with a human.
- **Data protection:** AI must comply with GDPR, confidentiality agreements and internal security standards.
- **Ethics and fairness:** AI must not introduce bias, misrepresent findings or misinform stakeholders.
- **Quality and accuracy:** AI outputs are reviewed to ensure reliability and are validated by human judgment.

4. Human Oversight and Decision-Making

AI tools provide **recommendations, flags, or drafts**; they do not make final decisions. A trained human will review AI outputs before results are used or shared. Any removal, exclusion, classification, or inclusion of data will **only occur after human approval**. For matters involving subjective interpretation (e.g., verbatim meaning, respondent intent), humans will remain the decision-makers....



5. Approved Areas of AI Use

Rigour Research may use AI in the following contexts:

5.1 Data Quality and Validation

- Detecting duplicates and near-duplicates
- Flagging inconsistent, illogical or low-quality responses
- Identifying suspicious IPs, mismatched time zones or unusual patterns
- Highlighting potential fraud or respondent misconduct

5.2 Verbatim Analysis and Coding Assistance

- Clustering or tagging open-ended responses
- Identifying recurring themes or terminology
- Suggesting draft codes or sentiment classifications
- Scoring clarity or coherence of responses

5.3 Survey Checks and Operational Efficiency

- Spotting contradictory logic or outliers
- Drafting internal summaries or reports for analyst refinement
- Identifying missing data or formatting anomalies
- Supporting data cleaning and structuring

5.4 Internal Business Support

- Drafting internal templates or documents (subject to review)
- Information retrieval, summarisation and research assistance
- Automating repetitive administrative processes

6. Prohibited Uses

AI must **not** be used to:

- Make final, automated decisions about data inclusion, exclusion or respondent removal
- Replace human review in any quality control process
- Generate deliverables for clients without human verification
- Handle personally identifiable information in unapproved or unsecured systems
- Create synthetic research findings without methodological oversight
- Circumvent ethical or legal standards



7. Human Oversight and Decision-Making

AI tools may inform, assist or flag, but they must not act alone. The following rules apply:

- All AI suggestions are reviewed by an appropriately trained human
- Analysts and project leads retain ownership of final decisions
- Any automated flagging must be validated before action is taken
- Reports generated with AI input must be checked before external use
- Escalation occurs where AI outputs contradict context or judgement

AI NEVER replaces human accountability.

8. Data Protection, Security and Confidentiality

- Client or respondent data must only be used in secure, approved platforms
- Personal data must be anonymised where possible
- No confidential data may be entered into public AI systems without explicit client approval
- All AI use is subject to ISO 27001 and GDPR standards
- Access is restricted to authorised personnel only

9. Training and Accountability

- Staff using AI tools receive appropriate guidance and training.
- Line managers ensure AI usage aligns with this policy.
- Any concerns or misuse must be reported to the Head of Operations or Data Protection Lead.

10. Continuous Review

This policy will be reviewed regularly to reflect:

- Advances in AI capabilities
- Evolving legal and ethical standards
- Client expectations and contractual requirements