

Artificial Intelligence (AI) Policy

Document Owner: Managing Director / Chief Technology Officer

Approved By: Board of Directors

Effective Date: 01.01.2026

Review Date: Annually or as required

1. Purpose

RSR Global Ltd. recognizes that Artificial Intelligence (AI) can significantly enhance productivity, innovation, customer service, and decision-making. This policy establishes the principles and rules governing the responsible, ethical, secure, and lawful use of AI technologies across the company.

The objectives of this policy are to:

- Encourage responsible innovation.
- Protect confidential and personal information.
- Ensure compliance with applicable laws and regulations.
- Minimize operational, legal, ethical, and cybersecurity risks.
- Maintain transparency and accountability in AI-assisted work.

2. Scope

This policy applies to:

- All employees
- Directors
- Contractors
- Consultants
- Temporary staff
- Third-party service providers using AI on behalf of RSR Global Ltd.

It covers all AI systems including:

- Generative AI (e.g., ChatGPT, Claude, Gemini, Microsoft Copilot)
- AI coding assistants
- AI image and video generation tools
- AI-powered analytics
- Machine learning models
- AI integrated into enterprise software

3. Guiding Principles

RSR Global Ltd. will ensure that AI is used in accordance with the following principles:

Lawfulness

AI must always be used in compliance with:

- UK GDPR
- Data Protection Act 2018

- Copyright legislation
- Employment law
- Contractual obligations
- Industry regulations

Human Oversight

AI supports—not replaces—human judgment.

Employees remain accountable for:

- Decisions
- Recommendations
- Communications
- Deliverables

Transparency

Employees should disclose AI assistance where appropriate, particularly when preparing:

- Client reports
- Professional advice
- Regulatory documents
- Public communications

Fairness

AI must not be used in ways that discriminate based on:

- Race
- Gender
- Religion
- Disability
- Age
- Sexual orientation
- Nationality
- Other protected characteristics

Security

AI must never compromise company security or client confidentiality.

4. Acceptable Use

Employees may use approved AI tools for:

- Drafting documents
- Research
- Brainstorming ideas
- Summarizing information
- Coding assistance

- Data analysis
- Translation
- Meeting summaries
- Presentation creation
- Process automation
- Knowledge management

All AI-generated work must be reviewed by the employee before use.

5. Prohibited Use

Employees must not:

- Upload confidential client information into public AI tools without approval.
- Upload personal data unless explicitly authorized and compliant with data protection requirements.
- Upload commercially sensitive information.
- Use AI to create fraudulent or misleading information.
- Generate fake identities or deceptive content.
- Produce discriminatory or offensive material.
- Use AI to bypass security controls.
- Generate malicious software or cyberattack tools.
- Rely solely on AI for legal, financial, medical, or regulatory advice without expert review.
- Present AI-generated content as verified fact without validation.

6. Data Protection

Before using any AI platform, employees must ensure they do not disclose:

- Client confidential information
- Financial records
- Passwords
- API keys
- Source code (unless approved)
- Intellectual property
- Trade secrets
- Employee personal information
- Customer personal information

Where possible, company-approved enterprise AI platforms with appropriate security controls should be used.

7. Intellectual Property

Employees remain responsible for ensuring AI-generated content does not infringe:

- Copyright
- Trademark
- Patent
- Licensing requirements

AI-generated materials should be checked before publication or commercial use.

8. Accuracy and Quality

AI systems may generate inaccurate or fabricated information.

Therefore:

- Verify facts.
- Validate references.
- Review calculations.
- Confirm legal statements.
- Test generated code.
- Ensure outputs meet professional standards.

AI output must never be accepted without review.

9. Client Communications

AI may assist in preparing client communications.

However:

- Final responsibility rests with the employee.
- Confidential information must be protected.
- Sensitive advice requires appropriate professional review.

10. Cybersecurity

Employees must:

- Use only approved AI applications.
- Enable multi-factor authentication where available.
- Report suspicious AI outputs.
- Never share credentials with AI tools.
- Follow the Company's Information Security Policy.

11. Responsible AI Development

Where RSR Global Ltd. develops AI solutions, the company will:

- Assess risks before deployment.
- Test for bias.
- Document model limitations.
- Maintain audit records.
- Monitor performance.
- Review security regularly.

12. Human Decision-Making

AI shall not make final decisions regarding:

- Employment
- Disciplinary action
- Recruitment
- Contract awards
- Financial approvals
- Regulatory compliance

without appropriate human oversight.

13. Training

RSR Global Ltd. will provide appropriate AI awareness and training covering:

- Safe AI use
- Data protection
- Prompt engineering
- AI risks
- Bias awareness
- Cybersecurity
- Ethical AI

14. Monitoring and Compliance

The Company may monitor the use of AI systems to ensure compliance with:

- Company policies
- Security standards
- Legal obligations

Misuse of AI may result in disciplinary action.

15. Reporting Concerns

Employees should immediately report:

- AI security incidents
- Data breaches
- Incorrect AI outputs causing business risk
- Ethical concerns
- Suspected misuse

to their line manager or the Information Security Officer.

16. Policy Review

This policy will be reviewed annually or whenever:

- Significant AI technologies are introduced.
- Regulatory requirements change.
- Business risks evolve.

17. Definitions

Artificial Intelligence (AI): Computer systems capable of performing tasks that normally require human intelligence.

Generative AI: AI systems capable of creating text, images, code, audio, or video.

Personal Data: Information relating to an identified or identifiable individual.

Confidential Information: Any non-public business information belonging to RSR Global Ltd. or its clients.

18. Approval

Compliance with this policy is mandatory for all personnel working for or on behalf of RSR Global Ltd.

Failure to comply may result in disciplinary action, termination of contracts, or legal action where appropriate.