Pointer

Our policies

Artificial Intelligence Policy

Pointer Ltd

Organisation: Pointer Ltd
Version No: 1.0
Date: 18th April 2025

PEACE OF MIND SINCE 1972

Scope

This policy applies to all colleagues, contractors, and third parties who develop, procure, manage or use AI tools or systems on behalf of Pointer Ltd.

Policy

This policy outlines the guidelines for the use of Artificial Intelligence (AI) tools within Pointer Ltd. The aim is to ensure responsible, ethical, and secure use of AI technologies. It ensures that all use of AI aligns with our company values, regulatory obligations, and stakeholder expectations.

Data Privacy and Security

AI tools must collect data in compliance with GDPR and other relevant data protection regulations. No private data or confidential information is to be submitted to AI tools. Personal data used in AI training or decision-making must be anonymized where feasible.

Legal and Regulatory Compliance

AI practices must align with all applicable laws and regulations, including intellectual property rights and consumer protections. Regular audits will be carried out to ensure compliance with evolving AI-specific legislation.

Ethical Guidelines

AI systems should be designed to avoid biases and ensure fair treatment of all individuals.

Decisions significantly affecting individuals must include human oversight. AI decisions should be explainable and transparent to users.
Discriminatory or biased use of AI is strictly prohibited.

Assessment and Monitoring

AI systems in active use will be reviewed regularly for accuracy, unintended bias, and performance.

IT Incident response procedures will be followed if AI systems cause harm or malfunction.

Continuous monitoring to ensure adherence to this policy.

Accountability and Governance

Prior to deploying any AI system, a risk assessment must be conducted, including ethical, legal, security, and operational risks. High-risk AI use cases must be escalated to the Security Governance Group.

Outputs generated by AI must be reviewed for originality and copyright compliance. Ownership of AI-generated content must be clarified in contracts and internal use cases.

Roles and Responsibilities

Role	Responsibility
Security Governance Group	Oversight of AI projects, risk approval, and policy enforcement
IT Department	Ensure AI tools comply with cybersecurity standards
Managers	Ensure team use of AI aligns with this policy

Role	Responsibility
Colleagues	Use AI responsibly and report issues or misuse

Training and Awareness

Pointer will provide training on AI tools and the policy to colleagues to ensure responsible use. We will also provide updates through toolbox talks about AI technologies and best practices.

Colleague Use

Colleagues may use AI tools (e.g., generative AI assistants) for productivity, coding, writing, and analysis—but only with approved tools and within confidentiality guidelines.

Sensitive or proprietary information must not be entered into public AI tools (e.g., ChatGPT, Bard) without anonymization and approval.

Continuous Improvement

We will regularly update this AI policy to reflect technological advancements and regulatory changes.

Colleagues and Contractors can feedback and provide suggestions to improve our AI practices through the Pointer Portal or Observe It Report It Form.

Monitoring

Pointer Ltd reserves the right to monitor the use of IT resources to ensure compliance with this policy.

Consequences

Violations of this policy may result in disciplinary action, up to and including termination of employment.