

Artificial Intelligence Policy



Introduction

1. Purpose

The purpose of this policy is to govern the development, deployment, and management of Artificial Intelligence (AI) technologies at River Bank. This policy aims to ensure that AI technologies enhance operational efficiency, improve customer experience, and maintain competitive advantage while adhering to ethical standards and regulatory requirements.

2. Scope

This policy applies to all departments and employees within River Bank. It covers all AI applications and systems used across the organization, including those aimed at optimising operations, innovating financial products, enhancing customer experiences, streamlining compliance and risk management, and supporting data-driven decision-making.

3. Responsibility

The AI strategy leader owns this policy, reporting to the AI Steering Committee comprising stakeholders from IT, data science, HR, and relevant business units. Each department involved in deploying or interacting with AI systems is responsible for adhering to this policy, and each department will identify and train AI Champions, who report to SteerCo.

4. Review Period

The policy should be reviewed annually or more frequently if significant changes in AI technology or business practices occur.

5. General Policy Statement

River Bank commits to using AI technologies that are responsible, transparent, and aligned with our core values of integrity and innovation. AI systems will be used to automate processes, enhance decision-making, and improve customer and employee experiences without compromising ethical standards or customer privacy.

5.1 AI Applications

AI applications at River Bank include, but are not limited to:

- Automated process optimization in operations such as QA, underwriting, and document generation.
- AI-driven insights for dynamic product development and market forecasting.
- Personalization of customer interactions through AI-driven analytics and virtual assistants.
- Compliance and risk management automation to ensure adherence to regulations like GDPR.

5.2 Data Handling

AI systems will initially handle internal policies, procedures, and proprietary data without access to personally identifiable information (PII) or sensitive customer data. This restriction will be reviewed based on the outcomes of pilot projects.

5.3 External Partnerships

River Bank will collaborate with external AI solution providers, including Fifty One Degrees for governance and risk consulting, and designing, building and launching AI solutions. River Bank also will deploy technology powered by global technology providers for AI models and cloud services.

All external relationships will be governed by strict contracts to manage risks and ensure compliance with our AI ethics and privacy standards.

Ethical AI Statement

Artificial Intelligence Policy

6. Ethical AI Use

9.1 Transparency

AI systems must operate transparently with mechanisms in place to explain decisions and processes, especially in customer-facing applications.

9.2 Accountability

Clear responsibilities must be defined for all AI-driven processes, with designated teams or executives accountable for each AI application.

9.3 Fairness and Non-discrimination

Continuous auditing and review are required to ensure AI algorithms do not result in biased outcomes. Measures must be taken to guarantee fairness in all interactions.

9.4 Privacy and Data Protection

All AI systems must comply with GDPR, the ISO 270001 accreditation and other data protection laws, with regular audits to ensure adherence.

9.5 Safety and Security

Robust security measures must be implemented to protect AI systems from cyber threats and unauthorised access.

9.6 AI Governance and Ethics Oversight

An AI Governance Board, an AI Ethics Officer, and Departmental AI Champions must be established to oversee and guide the ethical use of AI within River Bank.

7. Monitoring and Compliance

Monitoring tools and automated maintenance routines will be developed to ensure AI systems perform as intended and remain compliant with all regulations and ethical standards. Reporting will be integrated into the bank's enterprise risk management framework and the ISO270001 framework.

8. Incident Management

Protocols for incident management will be integrated with the bank's enterprise risk management framework and the ISO270001 ISMS to address and mitigate any issues arising from AI systems effectively.

9. Disciplinary Action

Violations of this policy can lead to disciplinary action, up to and including termination of employment. Specific penalties will depend on the nature and severity of the violation.

10. Relevant Documents

Additional guidance can be found in related policies on data protection, IT security, and human resources. Employees should also refer to the regulatory compliance guidelines provided by the PRA, FCA, and GDPR.