RESPONSIBLE USE OF ARTIFICIAL INTELLIGENCE (AI) POLICY

Document Details

Document Number			JT.IMS. P.14
Version:			28-Oct-2026
Date of Version:			00
Created by:	Jamilu Wamala	**Signature:**	
Reviewed By:	Ronald Awany	**Signature:**	
Approved By:	Paul Onek	**Signature:**	

Revision Record

Revision	Date	Responsible Person	Document Description
00	03.11.2026	Jamilu Wamala	Initial Version

Contents

1. Purpose and Scope 3
2. Definitions 3
3. Policy Statement 3
4. Policy Objectives 3
5. Legal and Regulatory Framework 3
6. Guiding Principles 4
7. Acceptable and Prohibited Use 4
8. Risk Classification 5
9. Data Protection, Third-Party Tools, and Development 5
10. Governance and Responsibilities 6
11. Risk Management, Incidents, Training, and Compliance 6
12. Review 6

1. Purpose and Scope

This policy governs the responsible use of Artificial Intelligence (AI) across Japotech Solutions Uganda Limited. It applies to all employees, trainees, interns, consultants, contractors, and business partners, as well as to every AI-powered tool, platform, model, or automation used or developed by or on behalf of Japotech.

It covers AI tools used across Japotech service lines including telecom site planning and installation, drive-test optimisation and network analytics, fibre and microwave link deployment, Network Operation Centre (NOC), apprenticeship training, digital marketing and all company operations including any Japotech client, partner, employee, or trainee data processed through AI. This policy operates in conjunction with Japotech's Human Resource, Data Privacy Policy, Information Security Policy, and Code of Conduct and Conflict of Interest policies.

2. Definitions

Artificial Intelligence (AI): a system that generates predictions, recommendations, content, or decisions using machine learning, rule-based, or generative techniques, in support of human-defined objectives.

AI Technologies and Tools: These include common AI tools used by Japotech team including ChatGPT, Perplexity, DeepSeek, Gemini and others.

3. Policy Statement

Japotech adopts AI technology as a strategic enabler of network performance, service quality, and operational efficiency while protecting data, respecting human rights, maintaining transparency with customers and staff, and upholding the standards certified under its ISO 9001 and ISO 45001 Integrated Management System. AI technology shall augment, not replace, the professional judgement of Japotech certified engineers, consultants, and trainers.

4. Policy Objectives

To promote ethical and transparent AI use; improve network, software, and customer service delivery through responsible automation; protect customer, employee, and company data; ensure compliance with applicable law and regulation; identify and mitigate AI-related risk; build staff and trainee AI capability; and preserve human accountability for every AI-assisted outcome.

5. Legal and Regulatory Framework

Japotech use of AI shall at all times comply with applicable Ugandan law and sector regulation, including the Data Protection and Privacy Act 2019 (and its Regulations, enforced by the Personal Data Protection Office), the Computer Misuse Act 2011, the Electronic Transactions Act 2011, Uganda Communications Commission (UCC) telecom regulations, the NITA-U Act 2009, the Employment Act 2006 (for AI in recruitment or performance management), and applicable intellectual property law. Where Japotech serves clients outside Uganda, the more stringent of local law, client contractual terms, or this policy shall apply. Japotech has regard to ISO/IEC 42001 (AI Management Systems) and ISO/IEC 27001 (Information Security), aligned with its existing ISO 9001/45001 certified management system.

6. Guiding Principles

1. **Human Oversight**: AI supports, never replaces, human judgment in decisions affecting customers, employees, network safety, or business commitments.

2. **Transparency**: Customers and staff are informed, in plain language, whenever AI materially such as a support chatbot shapes a decision or interaction.

3. **Fairness and Non-Discrimination**: AI is evaluated to minimise bias in company operations such as recruitment, training, admission, and customer-facing decisions.

4. **Privacy and Security**: All AI use complies with the Data Privacy Policy, the Data Protection and Privacy Act 2019, and Japotech's cybersecurity controls.

5. **Safety**: Where AI touches physical infrastructure, safety takes precedence over automation convenience, consistent with ISO 45001.

6. **Accountability**: Employees and management remain fully accountable for AI-assisted decisions and outputs; "the AI generated it" is not a valid defence.

7. Acceptable and Prohibited Use

Subject to the risk-tiering and approval process in this policy, AI may support service provisioning activities such as digital marketing, network planning, drive-test optimisation and radio network and microwave analytics; predictive maintenance and anomaly detection; assistance; NOC monitoring; first-line customer support chatbots (with escalation to a human agent); business reporting and analytics; technical documentation; apprenticeship and training content; and administrative process automation.

Acceptable Use	Prohibited Use
Employees may use approved AI tools for legitimate business purposes, including but not limited to: • Drafting emails, reports, presentations, and meeting minutes. • Research and information gathering. • Brainstorming ideas and improving productivity. • Creating summaries of non-confidential documents. • Software development assistance and code review. • Data analysis where approved and where sensitive information has been appropriately protected. • Translation and language enhancement. • Process automation and workflow improvement.	Employees shall not use AI systems to: • Upload or disclose confidential, proprietary, or classified company information unless expressly authorized and approved. • Input customer, employee, supplier, or partner personal information into public AI platforms. • Share passwords, encryption keys, financial records, network diagrams, security configurations, or sensitive operational information. • Generate misleading, fraudulent, defamatory, discriminatory, or offensive content. • Violate copyright, licensing agreements, or intellectual property rights. • Produce content intended to deceive customers, regulators, or other stakeholders.

All AI-generated outputs must be reviewed and validated by the user before they are relied upon or shared internally or externally.	• Make business, financial, engineering, legal, or regulatory decisions solely based on AI-generated recommendations without appropriate human review. • Circumvent company security controls or policies.

8. Risk Classification

Every AI use case is classified before adoption; the tier sets the required approval level.

Tier	Description	Minimum Control
Minimal	Negligible impact (e.g., writing help, internal search).	Standard acceptable-use rules.
Limited	Informs but doesn't replace decisions (e.g., code assistants, chatbots, drafting).	Human review; disclosure to users.
High	Materially affects network, customers, safety, finances, or employment.	Governance Committee approval, risk assessment, human-in-the-loop, and audit logging.
Unacceptable	Covert surveillance, social scoring, manipulative or unauthorised biometric AI.	Not permitted.

9. Data Protection, Third-Party Tools, and Development

a) Only data the user is authorised to access may be used with an AI system; personal data (customer, employee, trainee, or partner) is processed lawfully, fairly, and transparently under the Data Protection and Privacy Act 2019 and Japotech Data Privacy Policy.

b) Confidential or commercially sensitive network, site, and customer data must not be entered into public or unapproved AI tools; AI vendors must meet Japotech security requirements and sign a data processing agreement where they process personal data on Japotech behalf.

c) Every externally hosted or vendor AI tool must pass due diligence by the AI Governance Committee before use and, if approved, is added to the Approved AI Tools List maintained by the Head of ICT/Systems. Use of unapproved ("shadow") AI tools for company business is prohibited.

d) Where Japotech develops or customises AI-enabled systems (e.g., network analytics models, chatbots), it ensures documentation, data quality validation, model testing, a security assessment, ongoing performance monitoring, and human sign-off by the AI System Owner before deployment to live customer or network environments.

10. Governance and Responsibilities

Role	Responsibility
Managing Director	Ultimate accountability; approves high-risk AI initiatives.
Line Managers	Approve team-level AI use, monitor use, and escalate concerns. Technical/security evaluation of AI tools; maintains Approved AI Tools List. Ensures compliance with data protection law and policy.
All Staff, Trainees and Partners	Use only approved tools, verify outputs, protect data, and report incidents.

11. Risk Management, Incidents, Training, and Compliance

a) A documented risk assessment covering privacy, cybersecurity, operational/safety, legal/regulatory, ethical, and reputational risk is required before any Limited-risk-or-higher AI use case is implemented, and is logged in the AI Risk Register with an accountable owner and mitigation measures.

b) AI-related incidents (data breaches, biased or harmful outputs, security compromise, network misconfiguration caused by automated tools) are reported immediately via Japotech Incident Management Procedure and escalated to the Line Managers and Managing Director.

c) All staff receive role-appropriate AI awareness training covering this policy, safe prompting, data protection, and AI limitations; trainers ensure apprentices and trainees understand responsible-use expectations when AI tools are used in training delivery.

d) Non-compliance may result in disciplinary action under Japotech Human Resource policies; deliberate or repeated misuse involving customer data, network integrity, or safety may constitute grounds for summary disciplinary action.

12. Review

This policy shall be reviewed at least annually, or sooner where there are significant technological developments, regulatory changes, audit findings, or organisational changes affecting Japotech use of AI.