do UC AI Policy

Purpose

This policy defines how we adopt and use AI across our operations, products and services. It ensures our use of AI is responsible, safe, transparent and aligned with our strategic priorities. It applies to all employees, contractors and partners working under our direction.

This policy sits alongside, and does not replace, our **Privacy Policy**, **Information Security Policy**, contracts, or any applicable legal obligations.

1. Scope

This policy covers:

- All AI systems we build, buy or integrate
- All use of external AI tools (e.g. foundation models, domain-specific models, copilots)
- All automated, augmented or AI-assisted workflows
- Data used to train, prompt, evaluate or monitor AI systems
- All business functions, including product development, marketing, support, sales, operations and internal productivity use

2. Governance & Responsibilities

2.1 AI Owner / Responsible Officer

A designated senior leader is accountable for AI governance, supported by product, technical and operational leads.

2.2 AI Steering

Major AI use cases, new tools, or architectural changes require review by the AI Owner (or their delegate) before implementation.

2.3 Policy Review

This policy will be reviewed at least annually, or sooner if significant changes in capability, legislation or business risk arise.

3. Alignment with the AI Charter

All AI decisions and implementations must follow the principles defined in the AI Charter, including:

- Human-first purpose

- Accountable intelligence
- Responsible transformation
- Transparency
- Safety and reliability
- Data stewardship
- Fairness
- Workforce development
- Sustainable adoption
- Societal awareness

This policy operationalises those principles.

4. Red-Line Boundaries

AI must **never** act as the sole decision-maker for actions that materially affect people or businesses. This includes:

- Hiring, rejection, promotion, disciplinary actions
- Performance evaluation
- Pricing or contract terms
- Legal interpretation or advice
- Financial approvals and credit decisions
- Customer sanctions or risk decisions
- Decisions involving vulnerable individuals

Human judgement and documented oversight are mandatory for these decisions.

5. Acceptable Use of AI

5.1 Appropriate Use Cases

AI may be used for, for example:

- Productivity and task acceleration
- Drafting, ideation and summarisation
- Research support and synthesis
- Pattern recognition and analysis
- Customer, partner and internal support (with safeguards)
- Software development assistance
- Data validation, error detection and modelling
- Workflow automation where risk is low and outcomes are monitored

5.2 Inappropriate or Prohibited Use

AI may not be used for:

- Decision-making without appropriate human oversight

- Any activity requiring regulatory compliance checks unless the AI workflow is specifically approved for that purpose
- Entering or processing personal or sensitive data in unapproved tools
- Generating or modifying legal, contractual or financial documents without human review
- Automated actions that can initiate legal, financial or significant reputational risk without appropriate safeguards and approvals

6. Data Handling Requirements

Our use of AI must comply with:

- Our Privacy Policy and associated data-handling procedures
- All applicable data protection and privacy laws in the jurisdictions where we and our customers operate

6.1 Personal and Sensitive Data

Personal or sensitive data may only be used through approved systems that support compliant processing and appropriate safeguards.

6.2 Customer or Proprietary Data

Customer or proprietary data must not be entered into consumer or third-party AI tools unless explicitly approved and technically protected (for example, clear contractual terms on training rights and data usage).

6.3 Data Minimisation

Only the minimum necessary data should be used in any AI process.

6.4 Retention and Logging

Where AI systems store data or metadata, retention periods must be documented and aligned with our wider data-retention and privacy requirements.

7. Accuracy, Verification & Human Oversight

7.1 Verification Standard

All AI-assisted outputs — internal or external — must be verified by a competent human reviewer, to a level proportionate to the risk of the use case.

7.2 Material Outputs

Customer-facing or operationally critical outputs require heightened review, including for example:

- Technical recommendations or designs
- Migration or transformation plans

- Compliance-sensitive content
- Financial, legal, operational or risk-related outputs

7.3 Model Limitations

Employees must understand that AI may hallucinate, omit relevant information or generate factually incorrect or out-of-date content. AI output is an aid to judgement, not a substitute for it.

8. Workforce Development & Support

We commit to building human capability as AI capability expands.

8.1 AI Literacy by Role

We will provide appropriate AI literacy and support for each role category, not universal expertise. This may include training, guidance and access to safe experimentation environments.

8.2 Role Evolution

Where AI replaces tasks, we will seek to:

- Redeploy individuals to emerging roles where feasible
- Expand capability in AI operations, oversight and quality
- Avoid unnecessary or premature workforce displacement

8.3 Practical Skills Support

Employees will have opportunities to learn:

- Safe and effective prompting
- Quality checking and verification
- Critical evaluation of AI output
- Basic workflow integration
- Data responsibility when using AI tools

9. User Responsibilities & Awareness

We will remind and support users to:

- Use AI systems only for their intended business purposes
- Apply judgement and appropriate verification when relying on AI output
- Respect confidentiality, privacy and contractual obligations when using AI tools
- Escalate concerns about AI errors, misuse or unexpected behaviour to the AI Owner or relevant lead

Detailed behavioural expectations and any consequences of misuse are addressed in our wider employee guidance and handbooks, not in this policy.

10. AI Tool Approval Process

Before adopting a new AI tool or system, we will assess:

- Purpose and expected business value
- Security posture and data-handling (including data residency and any training/usage rights)
- Alignment with applicable data protection and privacy laws
- Operational and customer risk
- Integration and support requirements
- Monitoring and auditability

Tools that cannot meet minimum standards will not be approved for business use.

11. Monitoring, Quality Assurance & Incident Reporting

11.1 Monitoring

Key AI systems should be monitored for:

- Systematic errors or hallucinations
- Performance drift or degradation
- Misuse or unexpected patterns of use
- Potential data leakage or inappropriate outputs

11.2 Incident Reporting

Any issue that could create regulatory, privacy, customer, reputational or significant operational risk must be escalated promptly to the AI Owner (or delegate), following our incident or issue reporting processes.

11.3 Continuous Improvement

Feedback from employees, customers and internal audits should inform updates to models, workflows and governance practices.

12. Regulatory Considerations

Our approach will evolve in line with relevant global regulations and guidance, including for example:

- AI-specific legislation such as the EU AI Act, where applicable
- National and regional AI or digital regulation frameworks
- Sector-specific regulations applicable to our clients or partners

We will adopt or update controls as requirements and best practices evolve.

13. Policy Transparency

This policy may be shared externally to help partners and clients understand how we integrate AI into our businesses. It is not intended as legal advice or as an employee disciplinary policy.