Engagement Hub

ARTIFICIAL INTELLIGENCE (AI) POLICY

Security and AI

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	1/10/2024	Gillian Woolley	Document first created
0.1	1/7/2025	Gillian Woolley	Approved at MRM 1/7/2025

2 Document Contents Page

1 Document Version Control 2
2 Document Contents Page 3
3 AI Technology 4
3.1 Purpose 4
3.2 Scope 4
3.3 Principles 4
3.4 Approved AI Technology 4
3.5 AI Licencing 4
3.6 AI technology Risk Management 4
3.7 AI technology Supplier Selection 5
3.8 Locally Installed AI Technology 5
3.9 Changes to AI technology 5
4 AI Usage 5
4.1 Associated Policies 5
4.2 AI Usage Process Policy 6
4.3 AI Usage Table 7
5 Policy Compliance 9
5.1 Compliance Measurement 9
5.2 Exceptions 9
5.3 Non-Compliance 9
5.4 Continual Improvement 9

3 AI Technology

3.1 Purpose

The purpose of this policy is to manage and mitigate the risk of Artificial Intelligence (AI) to our organisation.

3.2 Scope

All employees and third-party users.

3.3 Principles

Use of Artificial Intelligence (AI) is in full compliance with legal, statutory, regulatory, and contractual requirements.

3.4 Approved AI Technology

Only company approved and licenced AI Technology is to be installed on company equipment or utilised.

Unauthorised AI technology must not be used.

A list of authorised AI Technology can be found in the Software Register.

See 4.3 for detail on permitted AI uses and how we improve privacy and accuracy when using AI software.

3.5 AI Licencing

AI Technology used by the organisation is acquired through official channels and where a purchase is required to use the AI Technology evidence of a valid license is retained.

AI Technology is used in line with the licencing agreement.

A software license register is maintained.

Software license reviews are conducted at least annually or after significant change.

3.6 AI technology Risk Management

AI technology is assessed for the risk to the organisation to information security before acquisition and usage.

Evidence of the risk assessment and risk management is recorded in the risk register.

3.7 AI technology Supplier Selection

AI technology selected is based on its ability to meet the needs of the business, including privacy and security obligations.

3.8 Locally Installed AI Technology

Where AI Technology is installed locally on organisation owned and managed technology:

- Patching levels are maintained in line with manufacturer recommendations.
- Only technology that is supported by the manufacturer is to be used.
- AI Technology is only installed by authorised, assigned persons.

3.9 Changes to AI technology

Changes to the AI technology used will follow the Change Management Policy and Change Management Process.

Changes to existing AI technology usage are significant changes and not to be taken lightly. This would be a significant change requiring a significant project with all associated resources and risk management and project management.

4 AI Usage

4.1 Associated Policies

All organisation information security policies apply to AI Technology as any other technology including but not limited to:

- Access Control Policy
- Risk Management Policy
- Information Classification and Handling Policy
- Logging and Monitoring Policy
- Secure Development Policy
- Patch Management Policy
- Intellectual Property Rights Policy

4.2 AI Usage Process Policy

AI Usage is approved by the Managing Director after a privacy impact assessment has been completed and assessed, if necessary for the type of information being used.

- Company data, internal data, confidential data, employee data or data of a sensitive nature cannot be input into AI Technology.
- AI Usage in the organisation is by an approval process.
- A register of approvals is maintained as part of the Software Register.
- A log of users is maintained.
- Users are educated periodically as part of the user training and awareness process on AI Technology usage including ethics, bias, non-discrimination, fairness, data privacy, intellectual property, and security.

The following table sets out the AI Usage in the Organisation.

4.3 AI Usage Table

Business Area	AI Allowed (Y/N)	Approved By	Usage Restrictions
Software Development	Y	Managing Director	AI **cannot** be used to produce code. All code created by AI must be separately checked for accuracy before use. AI **cannot** be used for testing. AI can be used to create product documentation. All copy created by AI must be separately checked for accuracy before publication/ use.
HR	N	Managing Director	AI **cannot** be used as part of any HR process or management process related to employees with the exception of the drafting of generic documentation. All copy created by AI must be separately checked for accuracy before publication/ use. No employee names or other identifying details may be used in AI systems.
Legal	N	Outsourced to third party Legal practice.	AI **cannot** be used as part of any Legal process.
Data Analytics	Y	Managing Director and Head of Marketing	AI **cannot** be used analyse employee data. All inputs must first be deidentified. AI **cannot** be used analyse customer data. AI **cannot** used analyse logging and monitoring data.

			AI **can** be used analyse web-based marketing monitoring such as Google Analytics data. AI **can** be used analyse capacity management data.
Social Media	Y	Head of Marketing	AI **can** be used to produce social media content. All copy created by AI must be separately checked for accuracy before publication/ use.
Marketing	Y	Head of Marketing	AI **can** be used to produce marketing content. All copy created by AI must be separately checked for accuracy before publication/ use.
Creation of Internal documents	Y	All Staff	AI **can** be used to produce internal documents. All copy created by AI must be separately checked for accuracy before use.
Creation of Public documents	Y	All Staff	AI **can** be used to produce documents for public use. All copy created by AI must be separately checked for accuracy before publication/ use.
Research – web based search for information.	Y	All Staff	AI **can** be used for research purposes. All copy/ references created by AI must be separately checked for accuracy before publication/ use.

5 Policy Compliance

5.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved and recorded by the Managing Director in advance and reported to the Management Review Team.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.