

Responsible Artificial Intelligence (AI) Policy

OHI Group Corporate Policy

Document Control	
Security Level	Public
Company	OHI Group
Department	CEO Office
Approved By	CEO
Date	July 2026
Revision	1.0

Contents

Responsible Artificial Intelligence (AI) Policy	1
OHI Group Corporate Policy	1
1. Policy Objectives	3
2. Scope	3
3. Our AI Commitment	4
4. Responsible AI Principles	4
4.1 Human Accountability	4
4.2 Transparency and Responsible Use	4
4.3 Data Protection and Privacy	4
4.4 Accuracy and Reliability	5
4.5 Fairness and Inclusion	5
4.6 Security	5
5. Approved Use of Artificial Intelligence	5
6. AI Governance and Accountability	6
7. Data Protection and Confidentiality	6
8. Human Oversight and Decision Accountability	6
9. AI Accuracy, Reliability and Validation	7
10. Intellectual Property and Ownership	7
11. AI Security Requirements	7
12. Third-Party AI Solutions	7
13. Employee Responsibilities and Awareness	8
14. Monitoring, Assurance and Continuous Improvement	8
15. Non-Compliance	8

1. Policy Objectives

Artificial Intelligence (AI) is transforming how organisations operate, innovate, and create value.

OHI Group recognises the potential of AI to improve productivity, enhance decision-making, strengthen operational performance, support innovation, and create sustainable value for our customers, employees, and stakeholders.

At the same time, AI technologies must be adopted responsibly, securely, and ethically.

This Responsible Artificial Intelligence Policy ("Policy") establishes the principles and minimum requirements governing the responsible use, development, implementation, and oversight of AI technologies across OHI Group.

The purpose of this Policy is to ensure that AI is:

- Used responsibly and ethically
- Aligned with OHI Group values and governance principles
- Secure and compliant with applicable laws and regulations
- Used to enhance human capability rather than replace human accountability
- Implemented with appropriate oversight and risk management

This Policy supports OHI Group's commitment to:

- Digital transformation
- Innovation and continuous improvement
- Information security
- Data privacy
- Responsible technology adoption
- Sustainable business practices

This Policy should be read together with:

- OHI Group Code of Ethics and Business Conduct
- Information Security, Data Privacy and Cybersecurity Policy
- Data Protection requirements
- Acceptable Use policies
- Relevant technology and digital governance procedures

2. Scope

This Policy applies across OHI Group, including all subsidiaries, controlled entities, business units, and operations.

It applies to:

- Board members
- Executive Leadership Team members
- Employees
- Contractors
- Consultants
- Temporary workers
- Suppliers and third parties using AI technologies on behalf of OHI Group

This Policy applies to all AI technologies, including:

- Generative AI tools
- Machine learning systems
- Automated decision-support tools
- Predictive analytics solutions
- AI-enabled software platforms
- AI solutions developed internally or provided by third parties

3. Our AI Commitment

OHI Group believes AI should be used as an enabler of human capability, innovation, and operational excellence.

We are committed to ensuring AI adoption:

- Creates value for our customers and stakeholders
- Supports our people and ways of working
- Protects confidential information and personal data
- Maintains professional judgement and accountability
- Supports safe, ethical, and responsible decision-making

AI will not replace the responsibility, expertise, and judgement of our people.

4. Responsible AI Principles

OHI Group applies the following principles when adopting and using AI.

4.1 Human Accountability

AI supports human decision-making but does not replace human responsibility.

Employees remain accountable for:

- Decisions made using AI outputs
- Reviewing AI-generated information
- Ensuring accuracy and appropriateness
- Applying professional judgement

AI-generated outputs must not be accepted without appropriate review.

4.2 Transparency and Responsible Use

AI must be used openly, responsibly, and appropriately.

Where AI contributes to significant business decisions, appropriate transparency should be maintained regarding:

- The use of AI
- The purpose of the AI application
- The role of human oversight

4.3 Data Protection and Privacy

AI solutions must protect personal data and confidential information.

Employees must ensure:

- Personal information is handled appropriately
- Confidential information is not entered into unauthorised AI tools
- Data is used only for legitimate purposes
- Information security requirements are followed

4.4 Accuracy and Reliability

AI outputs may contain errors or inaccuracies.

Employees must:

- Validate AI-generated content
- Verify facts and assumptions
- Apply professional expertise
- Correct inaccurate information before use

AI-generated outputs must not be relied upon blindly.

4.5 Fairness and Inclusion

AI solutions should be designed and used fairly.

OHI Group will seek to prevent:

- Unfair discrimination
- Bias
- Unintended negative impacts

4.6 Security

AI solutions must meet OHI Group cybersecurity requirements.

AI systems must consider:

- Access controls
- Data protection
- Supplier security
- Cybersecurity risks
- Regulatory obligations
-

5. Approved Use of Artificial Intelligence

AI may be used to support:

- Research and analysis
- Document drafting and review
- Data analysis
- Knowledge management
- Process improvement
- Productivity enhancement
- Innovation initiatives
- Operational optimisation

However, employees must ensure AI use remains consistent with:

- Company policies
- Customer obligations
- Confidentiality requirements
- Professional responsibilities

6. AI Governance and Accountability

Board of Directors

Provides oversight of significant technology and AI-related risks.

CEO and Executive Leadership Team

Responsible for:

- Supporting responsible AI adoption
- Ensuring appropriate governance
- Providing strategic direction

Digital Transformation / IT Function

Responsible for:

- AI governance framework
- Approved AI platforms
- Technology assessments
- Security requirements
- Supporting business adoption

Business Leaders

Responsible for:

- Identifying appropriate AI opportunities
- Ensuring responsible implementation
- Maintaining human oversight

Employees

Responsible for:

- Using AI responsibly
- Protecting company information
- Validating AI outputs
- Following this Policy

7. Data Protection and Confidentiality

Employees must not enter confidential, restricted, or sensitive OHI Group information into unauthorised AI platforms.

Examples include:

- Customer information
- Tender documentation
- Contractual information
- Employee records
- Financial information
- Engineering designs
- Proprietary information

AI tools must only process information appropriate to their approved purpose.

8. Human Oversight and Decision Accountability

AI must not be used as the sole basis for decisions involving:

- Employee matters
- Safety-critical decisions
- Contractual commitments
- Financial approvals
- Regulatory submissions
- Customer obligations

Qualified employees must review and approve decisions supported by AI.

9. AI Accuracy, Reliability and Validation

AI outputs must be reviewed before use.

Employees must consider:

- Accuracy
- Completeness
- Context
- Limitations
- Potential errors

AI-generated content must not be represented as expert advice unless validated by appropriately qualified personnel.

10. Intellectual Property and Ownership

Employees must protect OHI Group intellectual property when using AI.

Consideration must be given to:

- Ownership of AI-generated content
- Confidential information protection
- Customer intellectual property
- Third-party licensing requirements

11. AI Security Requirements

AI solutions must comply with OHI Group security requirements.

Security considerations include:

- Authentication
- Access management
- Data protection
- Secure configuration
- Monitoring
- Vendor assessment

12. Third-Party AI Solutions

Third-party AI solutions must be assessed before adoption.

Assessment should consider:

- Security controls
- Data handling practices
- Privacy compliance
- Contractual obligations
- Reliability
- Vendor reputation

13. Employee Responsibilities and Awareness

OHI Group will provide appropriate awareness and guidance to help employees use AI responsibly.

Employees must:

- Understand AI risks and opportunities
- Follow approved AI practices
- Protect company information
- Report concerns or misuse

14. Monitoring, Assurance and Continuous Improvement

OHI Group will monitor AI adoption through:

- Technology reviews
- Security assessments
- Compliance reviews
- User feedback
- Lessons learned

This Policy will evolve as AI technology, regulations, and business requirements develop.

15. Non-Compliance

Failure to comply with this Policy may result in:

- Removal of access to AI systems
- Disciplinary action
- Contractual consequences
- Further action where required