Unity Group Solutions Limited

Responsible AI Use Policy

Last updated: April 2026

1. Introduction

Unity Group Solutions Limited is committed to the safe, secure, responsible, and ethical use of artificial intelligence (AI). As a specialist consultancy operating at the intersection of cyber security and AI, and as the organisation behind the AI and Cyber Security Association (AICSA), we recognise both the transformative potential and the risks that AI presents.

This policy sets out our principles and commitments for the responsible use of AI in our own operations, in the services we deliver to clients, and in the guidance, we provide to the wider industry.

2. Scope

This policy applies to:

- All employees, contractors, consultants, and associates of Unity Group Solutions Limited.
- All use of AI tools, platforms, and systems in the delivery of our services.
- All content, training materials, and deliverables we produce.
- Any recommendations or guidance we provide to clients regarding AI adoption and use.

3. Our Principles

Our approach to AI is guided by the following principles:

3.1 Transparency

We are open and honest about how and where we use AI in our work. Where AI tools have been used in the creation of content, analysis, or deliverables, we will disclose this to clients and stakeholders where it is relevant to the context. We do not misrepresent AI-generated output as purely human work where transparency is important.

3.2 Human Oversight and Accountability

AI is a tool that supports human decision-making. It does not replace it. All AI-generated output used in our services is reviewed, validated, and approved by qualified human professionals before it is delivered or published. Ultimate accountability for the quality, accuracy, and appropriateness of our work rests with our team, not with AI systems.

3.3 Accuracy and Quality

We recognise that AI systems can produce inaccurate, incomplete, or misleading output. We take steps to verify the accuracy of any AI-assisted work and do not rely on AI output uncritically. We apply professional judgement, domain expertise, and editorial rigour to everything we produce.

3.4 Privacy and Data Protection

We do not input client confidential information, personal data, or sensitive business data into public or consumer AI tools unless explicit authorisation has been given and appropriate safeguards are in place. Where AI tools are used in the processing of personal data, we ensure compliance with the UK GDPR and the Data Protection Act 2018.

We assess the data handling and privacy practices of any AI tool before using it in the delivery of our services.

3.5 Security

We evaluate the security posture of AI tools and platforms before incorporating them into our workflows. We consider risks including data leakage, prompt injection, model manipulation, and supply chain vulnerabilities. We apply the same security standards to AI tools as we would to any other technology used in our operations.

3.6 Fairness and Bias

We are mindful of the potential for AI systems to reflect, amplify, or introduce bias. We take steps to identify and mitigate bias in AI-assisted outputs, and we do not use AI in ways that could result in discriminatory outcomes for individuals or groups.

3.7 Intellectual Property

We respect the intellectual property rights of others and do not use AI to reproduce, replicate, or derive content in ways that would infringe copyright or other intellectual property rights. Where AI is used in content creation, we ensure that the final output is original, appropriately attributed, and does not misappropriate the work of others.

3.8 Sustainability

We consider the environmental impact of AI use in our operations. Where possible, we choose AI tools and providers that are transparent about their energy consumption and are taking steps to reduce their environmental footprint.

4. Use of AI in Our Services

4.1 Content Creation

AI tools may be used to assist with research, drafting, editing, and ideation in the creation of content such as blog posts, articles, reports, and training materials. All AI-assisted content is reviewed, edited, and approved by our team before delivery or publication. The final output always reflects our professional expertise and editorial standards.

4.2 Security Awareness Training

Where AI tools are used in the development of training materials, scenarios, or simulations, we ensure that the content is accurate, relevant, and appropriate for the audience. We do not use AI to generate misleading or deceptive training content beyond the scope of agreed phishing simulation exercises.

4.3 Data Analysis and Reporting

AI tools may be used to assist with the analysis of data, such as phishing simulation results or programme metrics. Any insights or recommendations derived from AI-assisted analysis are validated by our team before being included in reports or presented to clients.

4.4 Client Advisory Work

When advising clients on AI adoption, governance, or risk management, we draw on our deep expertise in the intersection of AI and cyber security, including the frameworks and guidance promoted through the AICSA. Our advice is independent, evidence-based, and focused on helping clients use AI safely and responsibly.

5. Prohibited Uses of AI

We do not use AI for the following purposes:

- Creating deepfakes, synthetic media, or deceptive content intended to mislead.
- Processing personal data in violation of data protection legislation.
- Generating content that is discriminatory, harmful, or offensive.
- Surveillance, profiling, or monitoring of individuals without lawful basis and appropriate safeguards.
- Any use that would undermine the security, privacy, or rights of individuals or organisations.
- Replacing human judgement in decisions that have a significant impact on individuals.

6. Client Confidentiality

We take the confidentiality of client information seriously. We do not input client names, proprietary data, strategic plans, security assessments, or any other confidential client information into public AI platforms or tools unless we have explicit written authorisation from the client and have verified that the tool provides appropriate data protection guarantees.

Where a client engagement requires the use of AI tools that process client data, we will agree the scope, safeguards, and limitations with the client in advance.

7. Training and Awareness

All individuals who work for or with Unity Group Solutions Limited receive guidance on the responsible use of AI in their work. This includes understanding the capabilities and limitations of AI tools, recognising potential risks, and knowing when and how to escalate concerns.

8. Governance and Review

This policy is reviewed at least annually, or more frequently in response to significant developments in AI technology, regulation, or best practice. We monitor emerging guidance from bodies including the Information Commissioner's Office (ICO), the AI Safety Institute, the Department for Science, Innovation and Technology (DSIT), and international standards bodies.

Our work through the AI and Cyber Security Association (AICSA) ensures that we remain at the forefront of developments in AI governance and cyber security, and that our policies reflect current best practice.

9. Contact

If you have any questions about this policy or how we use AI in our services, please contact us at:

Unity Group Solutions Limited

Email: hello@unitysolutions.org.uk