**Governance** continued

# Cyber Security & Data Protection

Protecting company, customer and employee data remains a core governance priority for our organisation.

Our cyber security framework is designed to safeguard sensitive information, ensure operational resilience and support the secure use of technology across the organisation. We take a proactive, risk-based approach underpinned by strong governance, robust technical controls and a culture of shared awareness and responsibility.

### Security Monitoring and Resilience

We maintain continuous oversight of our IT environment through 24/7 monitoring and threat detection capabilities. This enables rapid identification and response to potential security incidents, supporting business continuity and reducing risk.

During 2025, we further strengthened our incident response processes, improving our ability to detect, assess and manage security events effectively.

### Building a Cyber Aware Culture

Employees play a critical role in maintaining a secure organisation. We continue to invest in cyber security awareness and training to ensure colleagues can identify and respond to potential threats.

In 2025, we introduced our first global Cyber Security Month, alongside the launch of our Cyber Heroes programme, recognising strong engagement and promoting shared accountability across the business.

Phishing simulation results in 2025 also continued to show improvement, with reduced susceptibility to phishing attempts and increased reporting across the organisation.

# Artificial Intelligence

AI is a rapidly evolving landscape, and like many organisations, we are continuing to assess how it can be applied effectively and responsibly within our business.

### AI Committee

During 2025, we established an internal AI governance committee to oversee the responsible and effective use of emerging AI technologies across the business. The committee brings together representatives from data and insights, marketing and business planning, ensuring a broad and balanced perspective aligned to the needs of our organisation and our stakeholders.

### AI Framework

As in every operational area of our business, we are taking a proactive approach to managing the opportunities and risks associated with AI, ensuring appropriate governance structures are in place as adoption increases.

As this work develops, our focus will be on formalising a clear framework to guide the use of AI across the organisation, supporting innovation while maintaining strong standards of control, accountability and data protection.

## Shaping Our Strategies

Gary plays a key role in shaping how emerging technologies are applied across the business, bringing a practical perspective to the work of the AI governance committee. His focus is on ensuring that digital innovation is aligned with business needs, while supporting the responsible and effective use of AI in operational and customer-facing environments.

**Gary Quinn**
Head of Digital Marketing

Scott leads the development and implementation of our cyber security strategy, ensuring that our systems, data and operations are protected through a combination of strong technical controls, governance frameworks and employee engagement.

**Scott Gilliland**
Head of IT