CYBERSECURITY STATEMENT

The Restaurant Group ("TRG") is committed to maintaining a cybersecurity programme designed to support the confidentiality, integrity and availability of its systems, services and information.

TRG recognises that cyber threats continue to evolve and, while no organisation can eliminate cyber risk entirely, TRG seeks to manage that risk through a proportionate, risk-based and continually reviewed set of security controls, processes and governance arrangements.

This statement provides a high-level overview of the cybersecurity measures that apply across TRG's directly controlled operations in the UK and Ireland. Individual divisions, brands or business units may implement additional controls or local procedures where appropriate, provided these remain consistent with TRG's overall security requirements. The statement describes TRG's general cybersecurity approach at a high level. It does not describe every control in place, and specific measures may change from time to time in line with risk, operational needs and legal or regulatory requirements.

SECURITY PRINCIPLES

TRG's cybersecurity approach is underpinned by the following principles:

- Governance and review: cybersecurity arrangements are subject to periodic review against recognised frameworks and internal governance requirements.
- Assurance: security controls are assessed through a combination of monitoring, review, audit and independent assurance activity, including technical testing where appropriate.
- Defence in depth: TRG maintains layered security controls across key areas such as network security, endpoint protection, identity and access management, and system administration.
- Vulnerability management: processes are in place to identify, assess, prioritise and remediate vulnerabilities and to support the timely application of security patches, taking account of risk and operational requirements.
- Incident preparedness: TRG maintains cyber incident response procedures intended to support the identification, escalation, containment, investigation and recovery of significant cyber incidents.
- Awareness and responsibilities: colleagues are expected to support cybersecurity through compliance with applicable policies, standards and awareness requirements.
- Third-party risk management: security considerations form part of TRG's due diligence and risk assessment processes for relevant suppliers, systems and services.
- Resilience and recovery: TRG maintains business continuity and disaster recovery arrangements, including the testing of recovery capabilities on a periodic and risk-based basis.
- Continuous improvement: TRG reviews and develops its cybersecurity arrangements over time in response to changes in technology, business operations, threat landscape and legal or regulatory expectations.

COMPLIANCE AND ACCOUNTABILITY

TRG expects all colleagues, contractors and other relevant users of its systems to comply with applicable cybersecurity policies, standards and procedures.

Suspected breaches of security requirements, or any actual or suspected cybersecurity incidents, must be reported through the appropriate internal channels without undue delay so that they can be assessed and managed promptly.

Non-compliance may be investigated and addressed in accordance with TRG's internal policies, contractual arrangements and governance processes.

EXCEPTIONS

Where a legitimate business need requires an exception to a TRG cybersecurity requirement, that exception must be subject to documented review, approval and periodic reassessment by the appropriate stakeholders.

Approved exceptions should be limited in scope, time-bound where possible, and supported by any compensating controls considered necessary to manage resulting risk.

Reviewed: July 2026
Approved by the TRG Board: 16 July 2026