UK Data Protection Compliance Policy

1. Purpose and Scope

This document describes the technical, organisational and procedural measures maintained by Newell's Projects Limited to support compliance with applicable UK data protection law, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, and to protect the rights and freedoms of data subjects.

2. Data Protection Governance and Accountability

- Maintain documented data protection, information-security and related operational policies and procedures.
- Allocate clear responsibility for data protection compliance, information security and incident management.
- Maintain appropriate management oversight, escalation and reporting arrangements.

3. Lawful, Fair and Transparent Processing

- Identify and document the lawful basis for processing personal data.
- Process personal data only for specified, explicit and legitimate purposes.
- Provide appropriate privacy information to data subjects explaining relevant processing activities, purposes, lawful basis, recipients, retention and rights.
- Where consent is relied upon, maintain appropriate mechanisms to record consent and enable withdrawal.

4. Technical and Information Security Measures

- Role-based access controls and least privilege principles.
- Network security controls, firewalls and endpoint protection.
- Malware, threat and security monitoring controls.
- Secure backup, restoration and disaster recovery arrangements.
- Physical security controls for offices, systems and equipment.
- Secure deletion, disposal and destruction of personal data and storage media.
- Periodic review of access rights, including prompt removal or amendment following role changes or departure.

5. Personnel, Confidentiality and Training

- Require personnel with access to personal data to comply with confidentiality obligations.
- Provide data protection and information-security training appropriate to individual roles.
- Maintain appropriate processes for onboarding, role changes and offboarding, including access removal.

6. Data Accuracy and Quality

- Collect only personal data that is adequate, relevant and necessary for the intended purpose.
- Use validation and quality checks where appropriate to support accuracy.
- Maintain processes enabling inaccurate or incomplete personal data to be corrected.
- Avoid unnecessary duplication of personal data and uncontrolled local copies.

7. Retention, Deletion and Secure Disposal

- Maintain appropriate retention schedules reflecting legal, regulatory, contractual and operational requirements.
- Retain personal data only for as long as necessary for the relevant purpose, subject to applicable legal requirements.
- Use secure deletion or destruction processes when personal data is no longer required.
- Apply appropriate controls to paper records, electronic records, removable media, devices and equipment.

8. Third-Party Suppliers and Processors

- Conduct proportionate due diligence before appointing third parties that process personal data.
- Assess suppliers' data protection, confidentiality and information-security arrangements according to risk
- Monitor supplier performance and compliance proportionately to risk.
- Ensure appropriate return or secure deletion of personal data at the end of a processing relationship, subject to legal requirements.

9. Business Continuity, Backup and Resilience

- Maintain appropriate business continuity and disaster recovery arrangements for systems processing personal data.
- Maintain backups appropriate to the criticality and risk of the information.
- Test restoration and recovery arrangements at appropriate intervals.

10.Physical Security

- Restrict physical access to premises and areas containing personal data or information systems.
- Secure paper records and portable equipment.
- Protect equipment against theft, loss, damage and environmental threats where appropriate.
- Apply secure disposal procedures to physical records and storage media.

11.Monitoring, Audit and Assurance

- Conduct periodic reviews of data protection compliance and information-security controls.
- Review user access rights and privileged access.
- Monitor training completion and awareness requirements.
- Review relevant supplier compliance.
- Review DPIAs and processing activities when circumstances change.

12.Continuous Improvement

The measures described in this document are reviewed and improved on an ongoing basis. Changes may be introduced in response to risk assessments, incidents, audits, testing, changes to processing activities, technological developments, contractual requirements or changes in applicable law and regulatory guidance.

This policy will be reviewed and published annually.

Signed on behalf of Newell's Projects Limited:

_____

D. M. Newell
Managing Director

Last Reviewed: Sept 2026