GENERAL DATA PROTECTION POLICY

Purpose

The purpose of this policy is to set out RED's approach to the handling of personal data and to ensure compliance with applicable data protection legislation.

RED is committed to processing personal data lawfully, fairly and securely, and to protecting the rights of individuals.

Data protection is a shared responsibility across RED, and all individuals are expected to understand and comply with their obligations under this policy.

RED has appointed a designated Data Protection Officer (DPO), the Group QSHE Manager, who is responsible for overseeing data protection compliance and providing guidance across the organisation. Queries relating to this policy or data protection matters should be directed to the HR function, who will liaise with the DPO where appropriate.

Scope

This policy applies to all employees.

It also applies to contractors, agency workers and any individuals who process personal data on behalf of RED.

This policy applies to personal data relating to employees, workers, applicants, contractors and former employees.

Key Definitions

Personal data means any information relating to an identified or identifiable individual.

Processing means any activity carried out on personal data, including collection, storage, use, disclosure or destruction.

Special category data includes information relating to health, race, religion, sexual orientation, political opinions and other sensitive data.

Criminal offence data relates to criminal convictions, offences or related proceedings.

Data Protection Principles

RED processes personal data in accordance with the following principles:

- data is processed lawfully, fairly and transparently
- data is collected for specified, explicit and legitimate purposes
- data is adequate, relevant and limited to what is necessary
- data is accurate and kept up to date
- data is retained only for as long as necessary
- data is processed securely and protected against unauthorised or unlawful access, loss or damage

RED will ensure individuals are informed about how their data is used through appropriate privacy notices.

Use of Personal Data

RED will only process personal data where there is a lawful basis to do so, including:

- where it is necessary for the performance of a contract
- where there is a legal obligation
- where there is a legitimate business interest, provided this is balanced against the rights and freedoms of the individual
- where another lawful basis applies under data protection legislation, including consent where this is genuinely appropriate

RED will only rely on consent where this is appropriate and can be freely given. In an employment context, other lawful bases will often be more appropriate depending on the nature of the processing.

Individual Rights

Individuals have rights in relation to their personal data, including the right to:

- access their personal data
- request correction of inaccurate data
- request erasure of data where appropriate
- restrict or object to processing
- request transfer of their data in certain circumstances

Requests should be submitted to HR.

RED will normally respond within one month, in line with legal requirements.

Data Security

RED takes the security of personal data seriously and has appropriate technical and organisational measures in place to protect it.

Personal data must only be accessed by individuals who are authorised to do so and for legitimate business purposes.

Where third parties process data on RED's behalf, appropriate contractual and security measures will be in place.

Personal data may be stored and processed using secure cloud-based systems and business applications. RED will ensure that appropriate security measures, access controls and contractual safeguards are in place when using third-party systems to process personal data.

Data Breaches

All data breaches must be reported immediately to the HR function. HR will ensure the matter is assessed and, where appropriate, escalated to the relevant internal function, such as IT or senior management.

Individuals remain responsible for reporting breaches promptly and must not attempt to investigate or resolve breaches independently.

RED will assess each breach and take appropriate action.

Where required, RED will notify the Information Commissioner's Office within 72 hours and inform affected individuals where there is a high risk to their rights and freedoms.

Individual Responsibilities

All individuals who have access to personal data are responsible for:

- accessing only the data they are authorised to access
- using personal data only for legitimate business purposes
- keeping data secure at all times
- not disclosing data without appropriate authorisation
- not storing personal data on personal devices or unsecured locations
- reporting any actual or suspected data breach immediately

Individuals must not access or use personal data for personal reasons or outside the scope of their role.

Individuals must not share personal data informally (for example, via personal messaging platforms or unsecured channels).

Failure to comply with these requirements may result in disciplinary action.

Serious or deliberate misuse of personal data may be treated as gross misconduct.

Manager Responsibilities

Managers are responsible for:

- ensuring employees understand and comply with this policy
- handling personal data in line with this policy and company requirements
- maintaining confidentiality of personal data shared with them
- ensuring data is only shared where appropriate and authorised
- reporting any data breaches immediately

Managers must seek guidance from HR where they are unsure how personal data should be handled.

Training

RED will provide appropriate training on data protection responsibilities.

Employees are expected to make reasonable efforts to understand and comply with their obligations.

Additional training may be provided where roles involve regular handling of personal data.

Breaches of this Policy

Failure to comply with this policy may result in action under RED's Disciplinary Policy.

Serious breaches, including unauthorised access, disclosure or misuse of personal data, may constitute gross misconduct and could result in dismissal.

Review

This policy will be reviewed periodically to ensure it remains compliant with current legislation and best practice.

It does not form part of any employee's contract of employment and may be amended at RED's discretion.