General Data Protection Regulation (GDPR) Policy

This policy sets out how the Company processes personal data in both manual and electronic records as part of its HR activities. It also outlines how the Company manages data breaches and upholds individual rights under the GDPR.

This policy applies to personal data relating to job applicants, employees, former employees, apprentices, and workers ("relevant individuals").

Personal data is information that identifies a person directly or indirectly.
Special category data includes information such as health, race, ethnicity, religion, sexual orientation, and biometric or genetic data.
Criminal offence data relates to convictions or alleged offences.
Processing refers to any action taken with personal data.

The Company is committed to ensuring all personal data is processed lawfully, securely, and in compliance with GDPR and domestic law. Where third parties process data on behalf of the Company, the Company will ensure they follow appropriate security and compliance standards.

1. Types of Data Held

The Company keeps personal data in personnel files and HR systems. Depending on the individual and employment status, the Company may hold:

- Medical or health information, including disability details, to meet legal obligations.
- Risk assessments required for legal compliance.
- Equal opportunities data (e.g., ethnicity, sexual orientation, religion).
- CV details such as employment history, qualifications, and references.
- Documentation confirming the right to work in the UK.
- Payroll information including bank details, tax codes, and National Insurance numbers.
- Employment information such as job titles, contracts, pay, hours, and benefits.
- Disciplinary and capability records.
- Performance information including appraisals and targets.
- Absence and leave records (annual leave, sickness, family leave).

- Training records.
- Emergency contact details.

Relevant individuals should refer to the Company's Privacy Notice for the purposes of processing, lawful bases, and retention periods.

2. Data Protection Principles

All personal data held by the Company will:

- Be processed lawfully, fairly, and transparently.
- Be collected for specific and legitimate purposes.
- Be limited to what is necessary.
- Be accurate and kept up to date.
- Not be retained longer than necessary.
- Be kept secure against unauthorised access, loss, or damage.
- Be transferred internationally only in line with GDPR safeguards.

Individuals also have GDPR rights, including:

- To be informed
- To access their data
- To have inaccuracies corrected
- To request erasure
- To restrict processing
- To data portability
- To object to processing
- To protections against automated decision-making and profiling

3. Company Procedures

To protect personal data, the Company:

- Assigns staff with responsibility for data processing and auditing.
- Maintains clear accountability for data management roles.
- Provides individuals with information about how their data is used and what to do if they believe data is compromised.
- Trains employees on confidentiality, data protection, and breach reporting.

- Maintains records of the personal data it holds, where it came from, and who it is shared with.
- Conducts risk assessments to identify and reduce vulnerabilities.
- Reviews and documents consent where required, ensuring it is freely given, specific, informed, and unambiguous.
- Maintains procedures for detecting, reporting, and managing data breaches.
- Understands its responsibilities when transferring personal data internationally.

4. Access to Personal Data

Relevant individuals have the right to know whether their data is being processed and to request access to it.

- Subject access request forms are available from HR.
- The Company will not charge for requests unless they are excessive, unfounded, or repetitive.
- The Company will respond within one month, with a possible two-month extension for complex cases.
- Individuals must notify the Company immediately if they believe any data is inaccurate.

5. Data Disclosures

The Company may disclose data where necessary, including:

- To providers of employee benefits.
- To support reasonable adjustments for disabled individuals.
- For health and safety or occupational health requirements.
- For statutory payments such as SSP.
- For HR management and assessing fitness for work.
- For insurance or pension administration.

Disclosures will only occur when required and proportionate.

6. Data Security

The Company uses technical and organisational measures to protect personal data.

Employees must:

- Store confidential files securely.
- Ensure sensitive information is not accessible to unauthorised persons.
- Keep data accurate.

- Use assigned passwords and keep them confidential.
- Use screen-locking to prevent unauthorised viewing.

Portable devices (laptops, USB drives, etc.) must not store personal data unless authorised. When permitted, data must be encrypted, stored only when necessary, and devices must be kept secure.

Failure to follow data security rules may result in disciplinary action, up to and including dismissal.

7. International Transfers

The Company does not transfer personal data outside the EEA.
Any future international transfers will comply with GDPR Chapter 5 (Art. 44–50).

8. Data Breach Notification

Where a breach is likely to risk individuals' rights and freedoms:

- The Company will notify the Information Commissioner within 72 hours.
- Individuals will be informed if the risk to them is high.
- Public communication will occur where legally required.

9. Training

- All new employees must read and understand data protection policies during induction.
- All employees receive training on confidentiality, data protection, and breach procedures.
- Staff with responsibility for data protection receive appropriate specialist training.
- Employees who use the computer system are trained on secure data handling.

10. Records of Processing

The Company maintains records of its processing activities, including purposes and retention periods. These records are kept up to date to ensure accuracy and compliance.