

GDPR Policy

1. Rainbow Health Resources Limited is committed to ensuring that all personal data is handled in compliance with the General Data Protection Regulation (GDPR). This document outlines the policies and procedures we follow to protect the personal data of our clients, staff, and care partners.

2. Data Protection Principles Rainbow Health Resources Limited adheres to the following GDPR principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

3. Types of Data Collected We collect and process personal and sensitive data, including but not limited to:

- Staff details: Name, contact information, employment records, DBS checks, training records.
- Client details: Name, health information, care plans, emergency contacts.
- Partner details: Contact persons, business details.

4. Lawful Basis for Processing We process personal data under the following lawful bases:

- **Consent** – When individuals explicitly agree to data processing.
- **Contractual necessity** – To fulfill service agreements with clients and staff.
- **Legal obligation** – Compliance with regulatory requirements.
- **Legitimate interest** – Ensuring safe and effective care services.

5. Data Subject Rights All individuals have the right to:

- Access their personal data.
- Request correction of inaccurate data.
- Request deletion of their data (“Right to be Forgotten”).
- Restrict or object to data processing.
- Data portability.
- Lodge a complaint with the Information Commissioner's Office (ICO).

6. Data Security Measures To ensure the protection of personal data, we implement:

- Secure digital storage with encryption.
- Limited access control to authorized personnel.
- Regular data protection training for staff.
- Secure disposal of physical and electronic data.

7. Data Breach Policy In case of a data breach:

- The breach will be assessed and contained immediately.
- The ICO will be notified within 72 hours, if required.
- Affected individuals will be informed where necessary.
- Remedial action will be taken to prevent future breaches.

8. Data Retention & Disposal We retain data only as long as necessary:

- Staff records: Up to 6 years after termination.
- Client records: 3 years after service completion.
- Financial records: 6 years.
- Data is securely disposed of when no longer required.

9. Third-Party Data Sharing We may share data with:

- Care homes and healthcare providers for service provision.
- Regulatory authorities when legally required.
- Third-party service providers with appropriate safeguards in place.

10. Staff Training & Accountability All employees receive GDPR training and are responsible for:

- Handling data securely.
- Reporting data breaches.
- Complying with this policy.

11. Contact Information For any GDPR-related inquiries, contact our Data Protection Officer (DPO) at: [Insert Contact Information]

12. Review & Updates This policy is reviewed annually or in response to changes in regulations.

Acknowledgment

All staff must acknowledge they have read and understood this policy.

Signature: _____ **Date:** _____

[Company Representative]