Helios Health Partnership

Privacy Policy for Staff and Potential Employees

1. Purpose of this Policy

This Privacy Policy explains how **Helios Health Partnership** ("we", "our", "us") collects, uses, stores, and protects personal information relating to our current and former employees, workers, contractors, and individuals applying to work with us ("you", "your").

We are committed to protecting your privacy and ensuring compliance with the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**.

2. Scope

This policy applies to:

- All **employees**, **workers**, **contractors**, and **consultants** engaged by Helios Health Partnership; and
- All **job applicants** and **potential employees**, including those applying directly or via recruitment agencies.

3. Information We Collect

a. Job Applicants

We may collect and process the following personal data:

- Full name, contact details, and address
- Curriculum vitae (CV), cover letter, and employment history
- Education and qualifications
- References and referee contact details
- Interview notes and assessment results

- Right-to-work documentation and identification (e.g. passport, visa)
- Criminal record information (where legally required or relevant to the role)

b. Employees, Workers, and Contractors

In addition to the above, we may collect:

- Personal and emergency contact information
- Date of birth
- Bank account details, national insurance number, and tax information
- Employment contracts and employment history with us
- Salary, benefits, and pension information
- Attendance, leave, and sickness records
- Performance, appraisal, and training information
- Disciplinary and grievance records
- CCTV footage
- IT system usage logs and security monitoring data

4. How We Use Your Information

We process your personal data to:

- Manage recruitment and selection processes
- Verify your identity, qualifications, and right to work in the UK
- Prepare employment contracts and manage onboarding
- Administer payroll, pensions, and benefits
- Monitor attendance, absence, and performance
- Support training, development, and career progression
- Ensure health, safety, and workplace security
- Manage disciplinary, grievance, or capability processes
- Comply with legal and regulatory obligations
- Maintain secure IT and communication systems

5. Legal Bases for Processing

Helios Health Partnership processes personal data under the following lawful bases set out in Article 6 of the UK GDPR:

- **Contractual necessity:** To perform or prepare an employment contract with you
- **Legal obligation:** To comply with employment, tax, or health and safety laws
- **Legitimate interests:** For effective business operations, HR management, and workplace safety
- **Consent:** Where you have given explicit consent, such as for optional background checks or data retention for future opportunities

Where we process special category data (e.g. health information, race, religion), this will be done under Article 9 of the UK GDPR and Schedule 1 of the Data Protection Act 2018 — for example, for employment law, health and safety, or equality monitoring purposes.

6. Sharing Your Information

We may share your data with trusted third parties, including:

- Payroll and pension providers
- HR software or benefits administrators
- Occupational health providers and healthcare professionals
- IT service providers and system hosts
- Recruitment agencies and referees (for applicants)
- Government bodies (e.g. HMRC, Home Office) where legally required

All third parties are required to process your data securely and only for the purposes we authorise.

7. Data Retention

- **Job applicants:** Personal data is retained for up to **12 months** after the recruitment process, unless you consent to a longer period for future opportunities.
- **Employees and contractors:** Personal data is retained for the duration of employment and for **6 years** after employment ends, in line with statutory and best practice requirements.

- Certain records (e.g. pension or health and safety data) may be retained longer where required by law.

8. Data Security

We apply appropriate technical and organisational measures to protect your personal data from unauthorised access, alteration, loss, or destruction. This includes password protection, secure servers, and limited access to authorised personnel only.

10. Your Rights

Under the UK GDPR, you have the right to:

- Access and obtain a copy of your personal data
- Request correction of inaccurate or incomplete data
- Request deletion of personal data where appropriate ("right to be forgotten")
- Object to or restrict certain types of processing
- Withdraw consent (where processing is based on consent)
- Lodge a complaint with the **Information Commissioner's Office (ICO)** if you believe your data has been mishandled:

- Requests should be made in writing to our Data Protection contact (details below).

11. Changes to This Policy

We may update this Privacy Policy periodically to reflect changes in law or company practice. The most recent version will always be available on Teamnet or provided upon request.