Data Protection Policy

Healthy Performance regards the security of personal information as an imperative part of our service and as such, we aim to set the highest standards of professionalism when dealing with employee and client data. As we collect personal data to provide our key services it is essential that we adhere to General Data Protection Regulation (GDPR) guidelines. All personal information will be dealt with professionally whether it is collected on paper or in electronic format. Since 2017, aside from health screening records, we now operate a paperless organisation to further reduce the possibility of any data protection issues. The following objectives will maintain our standards.

Organisational Responsibility

- Adhere to GDPR guidelines and meet our legal obligations to specify the purposes for which information is used
- Information must be accurate, kept up to date and not kept for longer than necessary for the purposes for which it is processed
- Information must not be transferred to another country without appropriate safeguards being in place
- Information must be made available to subjects of that information and subjects of that information must be allowed to exercise certain rights in relation to their personal information
- Maintain accreditation of Cyber Essentials Plus (externally audited process)
- Carry out quarterly penetration testing on all of our systems and resolving any issues within 7 days
- Ensure that it is easy for personal data to be removed from all systems upon employee/client request
- Collect and process appropriate information only to the extent that it is required operationally
- Continuously highlight our team's responsibility for following good information security practice
- Provide training to adhere and maintain awareness of GDPR guidelines and best practise
- Store paper based documents in a secure and safe environment which is locked at all times
- Password protect access to all personal, including employee information and relevant electronic documents
- Built all future software infrastructure with high levels of security and robustness aligned with best practise
- Ensure our internal systems can restrict any user access instantly, and at any time
- Ensure all external laptops have bitlocker codes and suitable anti-virus security
- To achieve ISO27001 by December 2020 to ensure we have a robust and externally verified structure

Team Responsibility

- To keep data securely whilst in their care, never leaving paper based records onsite
- To ensure all PC's are logged out when away from their working environment
- To never use unsecured networks at any time when using company equipment

- Not disclose data verbally or in writing, accidentally or otherwise to unauthorised third parties
- Raise any training issues with your line manager as soon as possible

Compliance

- Compliance with GDPR is the responsibility of all team members both individually and collectively
- Any deliberate or reckless breach of this policy may lead to disciplinary and/or legal proceedings
- Any individual who considers the policy has not been followed must alert a member of the Leadership Team immediately

Responsibility

It is the responsibility of each of our team to abide by this policy and continually adhere to our very high standards. As with all of our policies the Data Protection Policy will be assessed on an annual basis by the Leadership Team who has ultimate responsibility for monitoring progress and identifying areas that require attention.