DATA PROTECTION POLICY

1. INTRODUCTION

Green Park recognises its responsibility in respect of data privacy of every individual that comes into contact with the business and respects the rights of an individual over the processing of his or her data as a basic human right.

In response to the General Data Protection Regulation that came into force on 25th May 2018 together with the Data Protection Act 2018, and following Brexit, the adoption by the UK of the retained law version of that Regulation (together 'GDPR'), the business implemented a number of policies and processes that are designed to mitigate the risks that the business creates for others by holding their data.

2. PURPOSE AND SCOPE

This policy outlines the basic understanding of GDPR rights and principles for the individual as well as the responsibilities and procedures for all employees with regards to data and requests that arise regarding data.

As part of your contract of you will need to confirm that you have read, understand and will abide by the following data privacy policies and processes in all aspects of the performance of your work for the company and in doing so will respect the privacy of others.

3. WHO IS COVERED BY THE POLICY

This policy covers all individuals working for Green Park at all levels and grades, including senior managers, officers, directors, employees, contractors, sub-contractors, agents, secondees, voluntary workers, trainees, home employees, part-time and fixed-term employees and agency staff, (collectively known as Employees in this policy).

4. INDIVIDUAL RIGHTS

Green Park seeks to comply with the GDPR. This means:

The right to be informed - this policy details the information to be collected and how it will be processed and used. Your data and personal information will be fairly and lawfully processed.

The right of access - you are entitled to confirm that your data is being processed. You also have the right to see your data.

The right to rectification - you are entitled to have any inaccurate or incomplete personal data corrected. Where possible, any third parties that have access to such data should be informed by Green Park of any subsequent correction or addition.

The right to erase - also known as the "right to be forgotten". You are entitled to have your data erased and to prevent any further processing where:

- The use of your data is no longer necessary
- Where you withdraw any consent
- Where you object to the processing and no overriding legitimate interest exists
- Your data was unlawfully processed
- Your data has to be erased to comply with a legal obligation or court order

The right to restrict processing - you have the right to block further data processing in the following circumstances:

- Where you contest the accuracy of the data
- Where you have objected to processing, but a legitimate public interest may exist

- Where processing was unlawful, but you have requested restriction, not erasure
- Where Green Park no longer needs the data, but you require it to establish, exercise or defend a legal claim (this can include an employment-related claim).

In this situation, Green Park will continue to hold your data but cease to process it further. The business will continue to hold such data as is necessary to respect your request to prevent further processing.

The right to data portability - you have the right to request that electronic personal data provided by you to Green Park be provided by the business back to you in an open format (and free of charge) that allows such data to be readily transferred back to you or a third party. This can only be personal data related to you and not any data related to another party or employee.

The right to object - you have the right to object to any personal data used:

- As part of the performance of a task within Green Park or where done in a legitimate public interest or the exercise of an official duty.
- In direct marketing, including profiling.
- Any processing for scientific or historical research and statistical analysis.

Rights in relation to automated decision-making and profiling - you have the right not to be subject to a decision based upon an automated process where that decision has a significant (including legal) effect on you. In this situation, you are entitled to human intervention in the decision, to express your views and receive an explanation of the decision and have the right to challenge the decision.

The exceptions to this are where the process is necessary:

- To enter into a contract with the Organisation
- Where authorised by law, for example, to prevent fraud or tax evasion
- Where a data subject has already given your explicit consent under Article 9 (2) of the GDPR.

5. GDPR DATA PROTECTION PRINCIPLES

Under Article 5 of the GDPR, Green Park will comply with the following principles to ensure your data will be:

- Processed for limited purposes and not in any way incompatible with those purposes
- Adequate, relevant and will not be excessive
- Accurate
- Not kept for longer than necessary
- Processed in accordance with your individual rights
- Secure
- Not transferred to countries without adequate data protection

6. YOUR EXPLICIT AGREEMENT & CONSENT

As part of your employment, Green Park will collect and store of your data under GDPR in accordance with Article 6 (1)(b) and 6(1)(f) of the GDPR.

7. YOUR PERSONAL DATA

Green Park only holds personal data directly relevant to your employment. This data is collected from your first employment application, and your continuing employment, including, but is not limited to:

- Third-party employment references
- Employment reports or assessments, including performance reviews
- Disciplinary details, including informal or formal warnings
- Grievance procedures and outcomes
- Salary reviews, benefits records and expenses claims
- Health records
- Where required for your role Green Park may conduct enhanced criminal records checks under the Disclosure & Barring Service (DBS).

This information is only collected to assist Green Park in the smooth running of the business and to ensure compliance with other statutory responsibilities such as equal opportunities employment.

Your data may be disclosed within Green Park within the senior leadership team, human resources and/or your immediate manager. Your data will not be disclosed to your peers or any other employees that do not require access to the data to carry out their roles within the business.

8. MAINTAINING RECORDS

Green Park will take all reasonable steps to ensure that personal data held by the business is accurate and kept up to date. To ensure accuracy, employees will be asked every 12 months to check that their personal information held by the business is correct. As an employee, you should always contact human resources administration (HRAdmin@green-park.co.uk) should your personal information change for any reason, for example, a change of surname, home address or telephone numbers. Out of date information or information that is no longer required will be deleted once it is found to be no longer required or out of date.

9. SICKNESS & HEALTH RECORDS

For day-to-day management, Green Park needs to keep records relating to the personal sickness and health records of each employee. Such personal data will record any periods of sickness or health matters, detailing the length and nature of the issue and the outcome. These records will be used to assess the health and welfare of employees and to highlight any issues that may require further investigation. Such data will only be disclosed to management and will not be disclosed to fellow employees (except those employees within human resources who process such data). If for any reason you do not wish your health records to be kept, please contact HRAdmin@green-park.co.uk.

10. DATA SECURITY

Green Park is committed to the secure storage and, where undertaken, the secure transmission of employees' data. Only management and employees within the senior leadership team or human resources have access to such data. All such data is protected by physical security, such as locks, and technical security, such as usernames and passwords to access computer records and data. Such data is only disclosed on a "need to know" basis. To further ensure the security of such records, Green Park reserves the right to monitor and keep detailed log files and computer data analysis of all accesses to employees' data. Green Park also reserves the right to vet all employees who have access to such data in the course of their normal employment within the business.

If as an employee you have legitimate access to personal data and you pass or transmit the data within the business to another party or parties who in turn have the right to see such data, the following rules apply:

- If the data is transmitted by email, it must be sent in an encrypted form.

- If the data is transmitted via a network, it must be done using a secure network. Wherever possible such data should not be sent via a wireless network where the risk of interception is greater.
- Such data should not be kept within the email program on your PC after it has been sent or received. The data must be removed from the body of the email message or deleted from any temporary folders if sent as an attachment. Care should be taken at all times not to delete the original data source.
- If the data is to be faxed, ensure that the intended recipient knows in advance that the data is coming via fax and that they are standing by the fax machine to receive the data. Ensure that the fax number is correct. You should also confirm the safe receipt of the data by the recipient.
- If data is to be passed in hard copy form, it should be handed to the recipient personally. The recipient should ensure that the data is stored in a locked drawer or cabinet.

Parties with legitimate access to such data should not use any third parties who do not have the authority to view the data to send or receive the data on their behalf.

All employees are reminded that unauthorised attempts to gain access to such data or accessing such data are disciplinary offences, and in certain situations, may constitute gross misconduct leading to summary dismissal. Such breaches may also constitute a criminal offence under GDPR.

11. HANDLING REQUESTS FROM DATA SUBJECTS

The GDPR requires that a company responds to an individual's requests in respect to their data within 30 days. Failure to respond to a request within this period would be a breach under GDPR therefore it is imperative to handle these requests quickly and correctly.

Data Subjects have the right to:

- Request access to all personal data processed/held by Green Park concerning them (Data Subject Access Request – DSAR).
- Request the rectification of any data processed/held by Green Park concerning them (user rights request).
- Request the erasure of all personal data processed / held by Green Park concerning them (user rights request).
- Restrict the processing by Green Park of their personal data (user rights request).

12. HANDLING A DATA SUBJECT ACCESS OR USER RIGHTS REQUESTS

Green Park is committed to responding to data subject access requests and User Rights requests promptly. In accordance with the GDPR, the company does not charge a fee for handling the request. Our privacy policy states that:

- All subject access requests should be addressed to – DSAR@Green-park.co.uk
- All user rights requests should be addressed to – Userrights@Green-park.co.uk

On receipt of the request, Green Park will acknowledge the data subject access or user rights request confirming receipt to the data subject and setting the latest date by which a response will be sent.

All data subject access and user rights requests will be entered on the risk register which is reported to the leadership team at the monthly Management Meeting.

It is the responsibility of all Green Park employees to ensure that any Data Subject Access Request or User Rights request they receive directly is immediately forwarded to Userrights@Green-park.co.uk or DSAR@Green-park.co.uk as appropriate.

Individuals who telephone the company with a data subject access or user rights request must be advised that they are required to make their request in writing by sending it to Userrights@Green-park.co.uk or DSAR@Green-park.co.uk as appropriate.

Any data subject access and user rights requests that come into the business through other channels (paper, social media, shared mailboxes etc.) must be forwarded immediately to Userrights@Green-park.co.uk or DSAR@Green-park.co.uk as appropriate.

The only person(s) authorised to respond to data subject access requests and user rights requests on behalf of the company are CFO, Director of Systems and Operations and Compliance Manager.

No-one else in the business is authorised to respond to a data subject access request.

Any of the following activities by staff will result in disciplinary action being taken:

- Failure to forward a data subject access request to the correct email address immediately on receipt.
- Sending data directly to the data subject instead of dealing with the request through the appropriate company process.
- Attempting to delete, amend, erase or conceal data held on a data subject after receipt of a data subject access request.

The later could result in a criminal offence and would be considered as gross misconduct resulting in the immediate suspension of employment and/or an investigation which could result in the termination of employment.

The process for handling a subject access data request or user rights request can be found on the shared drive in the GDPR folder or requested from your manager.

13. DATA BREACH REPORTING POLICY

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

Personal data breaches can include but are not limited to:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

The GDPR requires that a company monitor data breaches and where a personal data breach has occurred, establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, then Green Park must notify the ICO within 72 hours of becoming aware of the breach.

It is the responsibility of all Green Park employees to report a data breach or suspected data breach as soon as they become aware of it. Data Breaches or suspected data breaches should be reported to the operations@green-park.co.uk and will be handled be either CFO or Operations and Compliance Manager.

Green Park's process for handling a Data Breach can be found on the shared drive in the GDPR folder. On reporting a breach or suspected breach, employees are required to complete an internal report which can be found on the shared drive in the GDPR folder.

14. EXTERNAL DATA PROCESSING

Where Green Park uses third parties to process data and provide services or administer schemes around such data, the business will take all reasonable steps to ensure that such third parties have in place their own data protection policies.

Green Park will have in place and regularly review individual contracts with all third-party data processors and will not use any third-party data processor that does not comply with the General Data Protection Regulation (GDPR) as a minimum standard.

15. BENEFITS SCHEMES

Where Green Park provides additional benefits such as health insurance and a pension scheme, the business will not make use of data collected by third parties administering the schemes where such data is not required for the day-to-day operation of the organisation. Green Park will provide employees with details of the information to be collected by these third parties and how it will be used. Furthermore, Green Park will seek permission for the collection and use of this data prior to collection.

16. EQUAL OPPORTUNITIES MONITORING

Green Park may collect information relating to ethnic origin, sex or disability as part of an equal opportunities policy. Green Park will ensure that any questionnaires relating to such information are accurate and that where possible, the results will identify employment trends within the business and not identify individual employees.

17. EMPLOYEE REVIEWS & APPRAISALS

Green Park will only collect data required for the day-to-day operation of the business.

18. DATA TRANSFERS OUTSIDE THE UK

If Green Park seeks to transfer data outside the UK or the European Economic Area. Such data will only be transferred to countries deemed to provide adequate data protection and where those countries are subject to an "adequacy decision" made by the UK government, where the UK government is satisfied that the countries have adequate and suitable data protection protocols in place. Furthermore, Green Park will obtain the prior consent of all employees whose data is likely to be transferred.

19. OTHER DISCLOSURES

Where Green Park wishes to disclose employee data for promotional, marketing or other business purposes (for example, incorporated into an advertisement or brochure), the consent of the employee will be sought in advance. The employee should also be told where the data will be published and how widely. The employee has the right to refuse any such request.

20. EMPLOYEE MONITORING

Green Park will inform all employees where employee monitoring is introduced or increased. The business will take reasonable steps to ensure that employee's privacy and autonomy are preserved. Green Park will take reasonable steps to ensure that specific details of personal conversations or correspondence are not accessed. However, retains the right to monitor the actual use business resources by employees.

21. CCTV MONITORING

Green Park reserves the right to introduce or extend the use of CCTV within the business premises for security purposes. Where this occurs, signs will be displayed on the premises to make it clear to staff and visitors that CCTV is being used.

CCTV will only be used for monitoring activity on the business premises.

Recorded images will be stored securely, with only authorised employees, and (where requested) the police will have access to them.

Recorded images will only be retained for as long as necessary or where the police or courts require evidence.

All CCTV equipment will be regularly inspected to ensure proper functioning.

22. RETENTION OF EMPLOYEE RECORDS

Green Park will retain employee records for the following periods:

- Application Form: for period of employment
- References: 1 year
- Payroll and tax information: 6 years
- Sickness records: 3 years
- Annual leave records: 2 years
- Unpaid/special leave records: 3 years
- Annual appraisal/ assessments: 5 years
- Promotions: 1 year from end of employment
- Transfers: 1 year from end of employment
- Training: 1 year from end of employment
- Disciplinary matters: 1 year from end of employment
- References provided: 5 years from provided or end of employment
- Summary of service: 10 years from end of employment
- Injury or accident at work: 12 years from end of employment

Green Park will ensure the safe and secure disposal of employee records that are no longer required.

23. CRIMINAL LIABILITY

Knowingly or recklessly disclosing the personal data of others without the express consent of Green Park can constitute a criminal offence.

24. DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

Green Park will carry out Data Protection Impact Assessments (DPIAs) where the business intends to use new technologies, platforms or software and the processing of the data is likely to result in a potentially high risk to the rights and freedoms of individuals.

Any DPIA should include the following:

- A description of the new process and the purpose behind it
- Assessment of necessity and proportionality of the data processing
- Assessment of risks to individuals
- The measures and security in place to address and minimise any such risk

The person in charge of this Data Protection Policy will conduct any required DPIAs.

25. IMPLEMENTATION

Effective from July 2023.

This policy will be subject to review, alteration and replacement in order to reflect the changing needs of the business and to comply with legislation. Any alterations will be communicated to you.

If you have any questions in relation to this policy, please contact your Line Manager.

26. DECLARATION

I acknowledge receipt of the Green Park Data Protection Policy. I confirm that I have read and agree to comply with the policy.

SIGNED the Individual

Dated