CIVIL ENGINEERING, CONSTRUCTION, LANDSCAPING

DATA PROTECTION POLICY

This policy document applies to your employment at GSJP South Ltd, Beacon Hill Farm, Old Wareham Road, Corfe Mullen, Dorset, BH21 3RZ and all other Organization sites that you may be asked to work at from time to time.

1. Your Individual Rights

The Organization complies with the General Data Protection Regulation (GDPR) and all the Articles of the Regulation, 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 personal 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 the Organization 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 personal data is no longer necessary

- Where you withdraw your consent

- Where you object to the processing and no overriding legitimate interest exists

- Your data was unlawfully processed

- Your data must 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 the Organization 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, the Organization will continue to hold your data, but cease to process it further. The Organization 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 the Organization be provided by the Organization 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 the Organization or where done in a legitimate public interest or in 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 Organization

- Where authorized by law, for example, to prevent fraud or tax evasion

- You have already given your explicit consent under Article 9 (2) of the GDPR.

2. GDPR Data Protection Principles

Under Article 5 of the GDPR the Organization will comply with the following principles to ensure your personal 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

3. Your Explicit Agreement & Consent

3.1 As part of your employment within the Organization, the Organization will seek your explicit consent to the collection and storage of your personal data under the General Data Protection Regulation (GDPR) in accordance with Article 6 (a) of the GDPR.

3.2 Furthermore, the Organization also relies upon Article 6 (b) of the General Data Protection Regulation (GDPR) - due to the contractual relationship between you and the Organization by virtue of your employment within the Organization, and under Article 6 (c) of the General Data Protection Regulation (GDPR) - due to the Organization's legal obligations to collect and process your employment data.

3.3 All employees should read this Policy and the attached Data Consent Letter and complete the attached Data Consent Letter and submit it to the Organization on or before 25th May 2018.

4. Your Personal Data

4.1 The Organization only holds personal data directly relevant to your employment. This data is collected as, and when required from your first employment application form and your continuing employment within the Organization, such information includes, but is not limited to:

i) Third-party employment references

ii) Employment reports or assessments, including performance reviews

iii) Disciplinary details, including informal or formal warnings

iv) Grievance procedures and outcomes

v) Salary reviews, benefits records and expenses claims

vi) Health records

vii) Where required for your role within the Organization, the Organization may conduct enhanced criminal records checks under the Disclosure & Barring Service (DBS).

4.2 This information is only collected to assist our personnel department in the smooth running of the Organization and to ensure that the Organization complies with other statutory responsibilities such as equal opportunities employment.

4.3 Your personal data may be disclosed within the Organization to those within the personnel department and management, including your immediate manager. Your personal 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 Organization.

5. Maintaining Records

The Organization will take all reasonable steps to ensure that personal data held by the Organization is accurate and kept up to date. To ensure accuracy, the Organization will ask employees every 12 months to check that their personal information held by the Organization is correct. As an employee you should always contact the personnel department 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 by the Organization once it is found to be no longer required or out of date.

6. Sickness & Health Records

For day-to-day management, the Organization 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 the personnel department who process such data). If for any reason you do not wish your health records to be kept, please contact your manager.

7. Data Security

7.1 The Organization is committed to the secure storage and where undertaken, the secure transmission of employees' personal data. Only management and employees within the personnel department 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 the Organization reserves the right to monitor and keep detailed log files and computer data analysis of all accesses to employees' personal data. The Organization also reserves the right to vet all employees who have access to such data in the course of their normal employment within the Organization.

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

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

2. 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.

3. 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 always be taken, not to delete the original data source.

4. 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 safe receipt of the data by the recipient.

5. 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.

7.3 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.

7.4 All employees are reminded that unauthorized 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 the General Data Protection Regulation (GDPR).

8. Data Breaches & Reporting

8.1 Where the Organization suspects that a data breach has occurred the Organization has a duty to report the breach to the Information Commissioner's Office (ICO) within 72 hours of discovery of the breach.

8.2 The Organization has a duty to report a breach if the breach is likely to result in a risk to the rights and freedoms of the individual(s) concerned, and where not acted upon is likely to have a significant detrimental effect on the individual(s) concerned, for example the data accessed could result in identity theft, loss of confidentiality or other significant loss.

8.3 Where any such breach is potentially of high risk to the individual(s) concerned, they too should be notified of the breach as soon as the Organization discovers the breach.

8.4 A breach of data includes the destruction, loss, alteration, unauthorized disclosure of, or access to personal data.

9. External Data Processing

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

9.2 The Organization will have in place and regularly review individual contracts with all third-party data processors.

9.3 The Organization will not use any third-party data processor that does not comply with the General Data Protection Regulation (GDPR) as a minimum standard.

10. Benefits Schemes

Where the Organization provides additional benefits such as health insurance and pension scheme the Organization 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 Organization. The Organization will provide employees with details of the information to be collected by these third parties, and how it will be used. Furthermore, the Organization will seek permission for the collection and use of this data prior to collection.

11. Equal Opportunities Monitoring

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

12. Employee Reviews & Appraisals

The Organization will only collect data required for the day-to-day operation of the Organization.

13. Data Transfers Outside the European Economic Area

If the Organization seeks to transfer data outside the European Economic Area such data will only be transferred to countries deemed by the European Commission to provide adequate data protection. Furthermore, the Organization will obtain the prior consent of all employees whose data is likely to be transferred.

14. Data Access & Disclosure

14.1 All prospective, current or past employees have the right to request access to data directly relating to them, which is held by the Organization. The Organization will provide such information free of charge, subject to the right to charge for further requests where such requests are duplicated or excessive. The Organization can request further information from the person making the request in order to provide accurate and relevant results and to check the identity of the person making the request. The Organization seeks to provide such information within 30 days of receiving a request. The Organization will provide the person making the request with the following information:

1. Whether they hold any information regarding them, and if they do:

2. Descriptions of that information.

3. What it is used for.

4. The type of third-party Organizations it is passed to.

5. Provide a breakdown of any technical terms or codes.

14.2 The information where reasonably possible will be provided in a hard copy or permanent electronic form.

15. References

The Organization will not disclose details of confidential references where to do so would disclose the identity of the author or where it may cause harm or detriment to the author.

16. External Disclosure Requests

16.1 Where employees receive external requests for the disclosure of data the following guidelines should be observed:

a. Verify the identity of the person requesting the information.

b. Be on the lookout for fraud or deception.

c. Seek a written request.

d. Check any telephone numbers where an oral request is received.

e. Inform your manager if any request appears suspicious.

f. Your manager or HR Department should also be contacted where the party requesting the data states that disclosure is required by law.

g. Remember that a duty is owed to the employee whose data is to be disclosed, seek their prior permission unless doing so would alert them to a criminal investigation.

h. If the disclosure of the data is non-routine where possible provide the employee in question with a copy of the data disclosed. A record of all non-routine data disclosures should also be kept.

17. Other Disclosures

Where the Organization 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.

18. Trade Unions

The Organization will only provide data to trade unions where the trade union is recognized by the employer. The data will be limited to name, job description and job location. The Organization will also give each employee a prior right to

object to the disclosure. Where any such data is provided for collective bargaining the data will not identify individual employees.

19. Employee Monitoring

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

20. CCTV Monitoring

20.1 The Organization reserves the right to introduce or extend the use of CCTV within the Organization's 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.

20.2 CCTV will only be used for monitoring activity on the Organization's own premises.

20.3 Recorded images will be stored securely; with only authorized Organization employees and (where requested) the police will have access to them.

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

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

21. Medical Testing

If the Organization undertakes any form of medical testing of employees such testing will only be undertaken for clear health and safety reasons, for assessing an employee's medical fitness for continued employment or to assess their entitlement to health benefits, such as sick pay. Prospective employees may be tested for similar reasons. The results of any testing required for a health or pension scheme shall not be given to the Organization.

22. Retention of Employee Records

22.1 The Organization will retain employee records for the following periods:

a. Application Form: for period of employment

b. References: 1 year

c. Payroll and tax information: 6 years

d. Sickness records: 3 years

e. Annual leave records: 2 years

f. Unpaid/special leave records: 3 years

g. Annual appraisal/ assessments: 5 years

h. Promotions: 1 year from end of employment

i. Transfers: 1 year from end of employment

j. Training: 1 year from end of employment

k. Disciplinary matters: 1 year from end of employment

l. References provided: 5 years from provided or end of employment

m. Summary of service: 10 years from end of employment

n. Injury or accident at work: 12 years from end of employment

22.2 The Organization 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 the Organization can constitute a criminal offence.

24. Date of Implementation

This policy is effective from 1st September 2019 and shall not apply to any actions that occurred prior to this date.

25. Questions

If you have any questions regarding this policy document and how it applies to you, including how to request access to your personal data, please consult your manager.

26. Data Protection Impact Assessments (DPIAs)

26.1 The Organization will carry out Data Protection Impact Assessments (DPIAs) where the Organization 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.

26.2 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 minimize any such risk

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

27. Data Protection Officer

Where required the Organization shall appoint the manager in charge of this Policy as the Organization Data Protection Officer. This will be a board level post. Where the current Policy manager does not have the required seniority, the Organization will either promote the manager to a board level post or appoint a current director to the post of Data Protection Officer.

28. Alteration of this Policy

This policy will be subject to review, revision, change, updating, alteration and replacement in order to introduce new policies from time to time to reflect the changing needs of the business and to comply with legislation. Any alterations will be communicated to you by your manager.

DATA CONSENT LETTER – PROVIDING YOUR CONSENT

I confirm that I have read the Data Protection Policy and have been made aware of my enhanced data protection rights under the General Data Protection Regulation (GDPR).

I hereby give my consent for the Organization to collect the following data subject to the Data Protection Policy and General Data Protection Regulation (GDPR).

(Please give your explicit consent by ticking the box next to each piece of data. The Organization only collects the data necessary for your employment.)

☐ Employment Application Form

☐ References

☐ Payroll and tax information

☐ Sickness and health records, where required

☐ Annual leave records

☐ Unpaid/special leave records

☐ Annual appraisal/assessments

☐ Promotions

☐ Transfers

☐ Training

☐ Disciplinary matters

☐ Summary of service

☐ Injury or accident at work

☐ CCTV, camera, webcam or other security data

☐ Driving data, including black box and Tachograph data, where applicable

☐ Trade union data

☐ Telephone, email, internet and intranet records and logs, where required

☐ Equal opportunities data

☐ Gender, race and disability-related data

☐ Benefits and expenses data

☐ Criminal records for enhanced DBS checks, where required

Authorisation Signed

George Parker

Director Date: 15.09.2021