SOUTHERN PROJECTS LTD

PROGRAM TO COMPLY WITH GDPR 2018 POLICY
Version 1.0 6th of October 2025

Contents

DATA PROTECTION PRIVACY NOTICE

This privacy notice tells you what to expect when we collect personal information from clients and potential clients.

Topics

1. What information do we collect about you?

We collect personal data about you including name and contact information if you:

- Contact us with an enquiry
- Ask us to provide a quotation for goods or services
- Place an order with us for goods or services
- Register for marketing communications
- Make use of our website. Website usage information is collected by using Cookies (see below)

We will only collect the information which is necessary for us to process to meet your expectations.

Where you place an order with us for services, we will require you to supply certain information so that we can meet our contractual obligations to you and comply with our legal obligations to you (including health & safety and accounting obligations).

2. How will we use the information collected about you?

We will use the information you provide to provide the services you have requested to you.

Our lawful basis for processing personal data belonging to clients are:

1. To comply with our contractual obligations (i.e. provide the service, collect payment)
2. To comply with our legal obligations (including tax and revenue record keeping, health & safety compliance)
3. In the event of any legal claims arising out of the services we provide
4. Our legitimate interests in marketing activities relating to commercial contacts and clients which include additional care, safety, maintenance and warranty information
5. Where we have active consent to send marketing materials to consumer contacts and clients

We do not transfer personal data to countries outside the EU.

If you enquire or request a quotation, we will keep your information for as long as is necessary to answer the enquiry or supply the quotation and then for 12 months in the event you decide to use our services.

If you place an order for our services, we will keep your information for the duration of the services and then for 6 years in the event of any legal proceedings. We may be required by a contract or by law to retain certain information for longer (e.g. warranty information or health and safety information).

We may seek your consent to keep information relating to a project we have completed on your behalf for a longer period so that we can use the information to demonstrate our competence and the quality of our work to other interested parties.

We may use images of a project we have completed on your behalf for advertisement purposes but we will ensure that you or any other person cannot be identified from the images used.

3. Marketing

As a business, we do not send marketing communications to contacts or clients.

We would always seek an individual's consent to send marketing materials.

4. Access to your information and corrections/changes

If you would like to know what information we hold about you please write to us using the contact details below. We will usually supply copies of the information held within 30 days of receiving your request.

Please notify us if any of the information we hold about you has changed or is incorrect, we will be happy to update this for you.

5. Third parties

We may need to provide certain third-party organisations with your information to provide our services.

We will only provide them with the information they require and will only permit them to use the information for the required purpose.

If any such third party has used your information for any other reason without your consent, please notify us using the details below and we will investigate the matter.

The third parties we anticipate sharing your information with include:

1. Third-party contractors and suppliers (e.g. subcontractors, courier services)
2. Authorisation bodies where we need to obtain consent and permissions to perform the services (e.g. local planning authorities, the Environment Agency)
3. Our accountants for tax and revenue accounting
4. HMRC for tax and revenue purposes
5. The Health and Safety Executive for the purposes of health & safety reporting and compliance

6. Cookies

Our website uses cookies, which are text files which record information about website use. Further information can be found in the cookie policy which is on our website.

7. Changes to our privacy notice

We keep this privacy notice under regular review and will post details of any changes below. This privacy policy was last reviewed on 18th Feb 2018

8. Complaints

We strive to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously.

If you think that our collection or use of information is unfair, misleading or inappropriate please bring it to our attention. We would also welcome any suggestions for improving our procedures. You may report any concerns regarding how we have handled your data to the Information Commissioner on 0303 123 1113 or by using this link https://www.ico.org.uk/concerns.

9. How to contact us

Company	Southern Projects Ltd
Name	Gavin Spurway
Position	Company Director
Contact Address	128a, Park Avenue, Widley, Waterlooville, PO7 5DP
Telephone	07919604759
Email	gavin@southern-projects.co.uk

10. Changes to this Privacy Notice

We have made the following changes to this Privacy Notice

Date	Change
6th October 2025	New Policy – Issued by Gavin Spurway – Managing Director Signature: 

DATA PROTECTION POLICY

You must read this policy because it gives important information about:

- the data protection principles with which the Company must comply;
- what is meant by personal information (or data) and sensitive personal information (or data);
- how we gather, use and (ultimately) delete personal information and sensitive personal information in accordance with the data protection principles;
- where more detailed privacy information can be found, e.g. about the personal information we gather and use about you, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;
- your rights and obligations in relation to data protection; and
- the consequences of failure to comply with this policy.

Introduction

1.1 The Company obtains, keeps and uses personal information (also referred to as data) about job applicants and about current and former employees, temporary and agency workers, contractors, interns, volunteers and apprentices for a number specific lawful purposes.

1.2 This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to our workforce. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

1.3 We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information relating to our workforce, and how (and when) we delete that information once it is no longer required.

1.4 The Company's data protection officer, Michael Lock, Managing Director is responsible for informing and advising the Company and its staff on its data protection obligations, and for monitoring compliance with those obligations and with the Company's policies. If you have any questions or comments about the content of this policy or if you need further information, you should contact the data protection officer.

Scope

1.5 This policy applies to the personal information of job applicants and current and former staff, including employees, temporary and agency workers, interns, volunteers and apprentices.

1.6 Staff should refer to the Company's *data protection privacy notice* and, where appropriate, to its other relevant policies including in relation to *internet, email and communications, monitoring, social media, information security, data retention and criminal record information,* which contain further information regarding the protection of personal information in those contexts.

1.7 We will review and update this policy at least annually in accordance with our data protection obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy to staff when it is adopted.

Definitions

criminal records information	means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;
data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
data subject	means the individual to whom the personal information relates;
personal information	(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;

processing information	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;
pseudonymised	means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;
sensitive personal information	(also known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

Data Protection Principles

1.8 The Company will comply with the following data protection principles when processing personal information:

1.8.1 we will process personal information lawfully, fairly and in a transparent manner;

1.8.2 we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

1.8.3 we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;

1.8.4 we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information are deleted or corrected without delay;

1.8.5 we will keep personal information in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the information is processed; and

1.8.6 we will take appropriate technical and organisational measures to ensure that personal information are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

Basis for Processing Personal Information

1.9 We will only process personal data where we have a legal justification for doing so, which will be set out in the Company's data protection privacy notice.

Sensitive Personal Information

1.10 Sensitive personal information is sometimes referred to as 'special categories of personal data' or 'sensitive personal data'.

1.11 The Company may from time to time need to process sensitive personal information. We will only process sensitive personal information if:

1.11.1 we have a lawful basis for doing so as set out above, e.g. it is necessary for the performance of the employment contract, to comply with the Company's legal obligations or for the purposes of the Company's legitimate interests; and

1.11.2 one of the special conditions for processing sensitive personal information applies.

1.12 The Company's *data protection privacy notice will* set out the types of sensitive personal information that the Company processes, what it is used for and the lawful basis for the processing.

Criminal Records Information

1.13 Where we are required by law to carry out criminal record checks then we will do so and the information received will be used to make the appropriate recruitment / employment decision and then destroyed. We will not retain criminal records information for any more than 6 months.

Privacy Notice

1.14 The Company will issue privacy notices from time to time, informing you about the personal information that we collect and hold relating to you, how you can expect your personal information to be used and for what purposes.

1.15 We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Individual Rights

1.16 You (in common with other data subjects) have the following rights in relation to your personal information:

1.16.1 to be informed about how, why and on what basis that information is processed—see the relevant data protection privacy notices;

1.16.2 to obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request—see the Company's subject access request policy;

1.16.3 to have data corrected if it is inaccurate or incomplete;

1.16.4 to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');

1.16.5 to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal information but you require the data to establish, exercise or defend a legal claim; and

1.16.6 to restrict the processing of personal information temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation's legitimate grounds override your interests).

1.17 If you wish to exercise any of these rights please contact the data protection officer.

Individual Obligations

1.18 Individuals are responsible for helping the Company keep their personal information up to date. You should let the Company know if the information you have provided to the Company changes, for example if you move house or change details of the bank or building society account to which you are paid.

1.19 You may have access to the personal information of other members of staff, suppliers and customers/clients of the Company in the course of your employment or engagement. If so, the Company expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they may also enjoy the rights set out above.

1.20 If you have access to personal information, you must:

1.20.1 only access the personal information that you have authority to access, and only for authorised purposes;

1.20.2 only allow other Company staff to access personal information if they have appropriate authorisation;

1.20.3 only allow individuals who are not Company staff to access personal information if you have specific authority to do so from the data protection officer;

1.20.4 keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in the Company's *information security policy*);

1.20.5 not remove personal information, or devices containing personal information (or which can be used to access it), from the Company's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and

1.20.6 not store personal information on local drives or on personal devices that are used for work purposes.

1.21 You should contact the data protection officer if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

1.21.1 processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the lawful conditions being met;

1.21.2 any data breach as set out below;

1.21.3 access to personal information without the proper authorisation;

1.21.4 personal information not kept or deleted securely;

1.21.5 removal of personal information, or devices containing personal information (or which can be used to access it), from the Company's premises without appropriate security measures being in place;

1.21.6 any other breach of this policy or of any of the data protection principles set out in paragraph 1.8 above.

Information Security

1.22 The Company will use appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Storage and Retention Of Personal Information

1.23 Personal information (and sensitive personal information) will be kept securely in accordance with the Company's obligations.

1.24 Personal information (and sensitive personal information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained.

1.25 Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

Data Breaches

1.26 A data breach may take many different forms, for example:

1.26.1 loss or theft of data or equipment on which personal information is stored;

1.26.2 unauthorised access to or use of personal information either by a member of staff or third party;

1.26.3 loss of data resulting from an equipment or systems (including hardware and software) failure;

1.26.4 human error, such as accidental deletion or alteration of data;

1.26.5 unforeseen circumstances, such as a fire or flood;

1.26.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

1.26.7 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

Training

The Company will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Consequences Of Failing To Comply

1.27 The Company takes compliance with this policy very seriously. Failure to comply with the policy:

1.27.1 puts at risk the individuals whose personal information is being processed; and

1.27.2 carries the risk of significant civil and criminal sanctions for the individual and the Company; and

1.27.3 may, in some circumstances, amount to a criminal offence by the individual.

1.28 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

1.29 If you have any questions or concerns about anything in this policy, do not hesitate to contact the data protection officer.

Signature on behalf of Southern Projects Ltd

Signature: 
Name: Mr Gavin Nicolas Spurway
Position: Managing Director
Date: 6th of October 2025
Review Date: 6th of October 2026

The review period is a maximum of not more than 12 months.

DATA PROTECTION PRIVACY NOTICE TO EMPLOYEES

1. Purpose

This document sets out the type of information we will collect about employees, why we collect it and what each employee's rights are in relation to this data. This notice should be read in conjunction with the Company's Data Protection Policy.

2. Personal data we will collect and why

The table below sets out the type of data we collect from employees and the reason why we do so.

Data	Reason
Previous employment and educational information including references	In order to make informed recruitment decisions for the benefit of the Company
Contact information, e.g. address telephone number, email address	In order that we can contact you for reasons relating to your employment, e.g. organisation of work, providing information about your employment and pay
Bank account and details	In order that we can pay you your salary etc.
National insurance number	In order that we can process PAYE deductions and report to HMRC
Emergency contact details	In order that we can contact a family member or friend in the event of an emergency relating to the employee
Passport / birth certificates / visas etc.	In order to comply with our legal duty to check that all employees are entitled to work in the UK
Information relating to gender, age, race and ethnic/national origins, sexual orientation, religious or	In order to monitor equality and diversity within our workforce. Such information will normally be recorded in anonymous statistical format in order that it cannot be related to a specific individual

philosophical beliefs and marital status (1)	
General health information (1)	In order that we can effectively respond to illness or injury at work, make adjustments to your role/workplace
Short term health information e.g. fitness for work notes, absence records, accident reports (1)	In order that we can effectively manage absences, process statutory sick pay and ensure employees are fit to return to work To comply with our statutory accident reporting duties
Medical records and reports (1)	In order to manage a serious health issue which is affecting your employment
Criminal record and DBS disclosures (2)	In order to assess an individuals suitability for employment and, where it is a legal requirement to carry out DBS disclosures, comply without our obligation to do so
Performance and conduct information, e.g. training records and certifications, appraisal and disciplinary records and letters	In order to effectively manage an employee's performance and conduct at work and in order to defend legal proceedings

1 This type of data is classified as a special category of data. This means that you must expressly consent to the Company using this data and therefore we will explain the precise reason for collecting it at the time.

2 Where we carry out a criminal records or DBS disclosure we will use the information received to make our recruitment/employment decision and then destroy the information. We will not keep Criminal Records Information for more than 6 months

3. Storage of information

Employee information will be stored:

- In electronic format; and/or
- In hard copy format

Personal data stored in electronic format will be stored within computer or cloud based systems which are password protected. Access to information will be limited to those members of the Company who require access to it in accordance with the reasons set out in section 2 above.

Personal data stored in hard copy will be stored in locked filing cabinets, storage cupboards or offices with access limited to those members of the Company who Access to information will be limited to those members of the Company who require access to it in accordance with the reasons set out in section 2 above.

4. Third parties

It may be necessary for the Company to share some employee personal data with third parties. Where it does share personal data with a third party the Company will take measures to ensure that:

- the security of the personal data is maintained; and
- that it is not used unlawfully.

Circumstances where personal data may be shared include:

- With a third party payroll or pension provider in order to process wage payments and pension contributions
- With HMRC for PAYE purposes
- With employment law and HR advisors in order to obtain advice in relation to any contractual or legal employee relations issue
- In order to obtain a criminal records or DBS disclosure
- In order to provide employment references
- In order to comply with our statutory reporting duties to HMRC, the Health and Safety Executive etc.

If you consider that any third party has unlawfully used your personal data then you should notify the Company as soon as possible in order that we can investigate the matter and take steps to protect your personal data.

5. Updating your personal data

We are required to update personal data to ensure it is accurate and up to date. Therefore if any of your details change then you must notify us promptly of the change.

6. Accessing your personal data

You have the right of access to the personal data we have possession of, subject to certain legal limitations (e.g. in order to protect the rights and freedoms of other individuals).

If you wish to access your personal data then you should submit a written subject access request which:

1. Identifies who you are (we may seek confirmation of identity); and
2. States what personal data you wish to access

We will normally comply with subject access requests within one month of receiving the request unless it is a complex request.

Subject access requests should be made using the contact details below.

7. Deletion of personal data

We will delete personal data once we no longer have a lawful reason to hold and use it, unless you ask us not to delete it.

You have the right to have personal data deleted in certain circumstances. If you wish for personal data to be deleted then you should contact us in writing setting out what data you wish to be deleted. Requests should be submitted using the contact details below

8. Complaints

Any complaints in relation to the Company's use of your personal data should be addressed to the contact below or through the Company's grievance procedure. You may also report data protection concerns to the Information Commission on 0303 123 1113 or by using this link:

https://www.ico.org.uk/concerns.

9. Contact information

Name	Gavin Spurway
Position	Managing Director
Address	128a, Park Avenue, Widley, Waterlooville, PO7 5DP
Phone	07919604759
E.mail	gavin@southern-projects.co.uk

If you wish to make a subject access request, ask for data to be deleted or make a complaint about data protection then please do so in writing to:

Signature on behalf of Southern Projects Ltd

Signature: 
Name: Mr Gavin Nicolas Spurway
Position: Managing Director
Date: 6th of October 2025
Review Date: 6th of October 2026

The review period is a maximum of not more than 12 months.

SUBJECT ACCESS REQUEST FOR INFORMATION

1 Introduction

1.1 Where the Company processes personal data regarding an individual, that individual has the right to request copies of the personal data from the Company.

1.2 This request is known as a Subject Access Request.

1.3 Any Subject Access Request received by the Company will be dealt with in accordance with this policy.

1.4 This policy also covers the process to be followed where an individual requests that personal data be deleted or the processing of the data restricted.

2 Procedure

2.1 A Subject Access Request or request for deletion/restriction does not need to be in a specific format but must be in writing.

2.2 Any Subject Access Request or request for deletion/restriction should be directed to the MD for processing.

2.3 Before responding to a the request the identity of the person making the request should be confirmed. This may be done by speaking to the individual directly or cross referencing contact information such as postal or email address to ensure the data is not sent to the wrong person.

2.4 Data to be supplied may be sent in either hard copy or electronic format. Where it is sent in hard copy format, an inventory of the data sent should be made and stored on the individuals file to demonstrate compliance.

2.5 Data should be sent within 30 days of receiving the request. If it is not possible to supply all data within this time frame then the individual should be notified of this before the 30 day period expires with an explanation and estimated time scale for completion of the request.

2.6 Where there is any uncertainty about processing the request then advice should be sought from the Information Commissioner's Office or a relevant professional.

3 What data should be supplied

3.1 All data relating to the individual should be supplied as long as it falls within the scope of the next section and one of the exemptions at section 4 does not apply.

3.2 For data to be supplied it must relate to the individual and must be either processed automatically (e.g. data processed using a software application such as pay roll information or through a customer relationship management application) or be stored in a relevant filing system.

3.3 A relevant filing system may include:

3.3.1 Dedicated and organised personnel file

3.3.2 Dedicated client or job file

3.3.3 Data stored within a information management system which can be filtered by individual

3.3.4 Email folders where emails are categorised by individual or job

4 Exempt data

4.1 The following data is exempt from being supplied:

4.1.1 Data which does not relate to the individual

4.1.2 Data which is not processed automatically or stores in a relevant filing system (in particular it is not necessary to review all emails which reference the individual unless they have been categorised)

4.1.3 Data which includes information about other individuals unless that individual has consented to the supply of the data or the information can be suitably redacted

4.1.4 Legally privileged data; e.g. correspondence with legal or financial advisors in relation to the individual for the purposes of obtaining advice

4.1.5 Employment references **given** in confidence

4.1.6 Information which is already publicly available

4.1.7 Management information where disclosure would prejudice the Company (e.g. tender information or redundancy proposals prior to consultation commencing)

5 Fees

5.1 The Company will not charge an individual for complying with a Subject Access Request unless the request is manifestly unfounded or excessive in which case a reasonable fee may be charged.

5.2 We may charge the actual cost for supplying duplicate copies of data already supplied.

6 Deletion of data

6.1 All data subjects have the right to request for their personal data which the Company holds to be deleted.

6.2 Any such requests must be confirmed in writing by the data subject.

6.3 All such requests must be considered but do not need necessarily need to be accepted. A review should be carried out of the request to determine whether or not the Company has lawful grounds to continue to hold and process the data. These may include:

6.3.1 In order to comply with our contractual obligations

6.3.2 In order to comply with our legal obligations

6.3.3 In anticipation of a legal claim to which the data is relevant

6.3.4 Where our legitimate interests in processing the data outweigh those of the data subject to request its deletion

6.4 Further professional advice should be sought if necessary.

6.5 Any refusal to delete data should be confirmed in writing to the data subject, setting out the grounds of refusal.

7 Restriction on data processing

7.1 All data subjects have the right to request that any processing of their personal data which the Company holds to be restricted or stopped.

7.2 Any such requests must be confirmed in writing by the data subject.

7.3 All such requests must be considered but do not need necessarily need to be accepted. A review should be carried out of the request to determine whether or not the Company has lawful grounds to continue to process the data. These may include:

7.3.1 In order to comply with our contractual obligations

7.3.2 In order to comply with our legal obligations

7.3.3 In anticipation of a legal claim to which the data is relevant

7.3.4 Where our legitimate interests in processing the data outweigh those of the data subject to request its deletion

7.4 Further professional advice should be sought if necessary.

7.5 Where possible the processing of the data should be temporarily suspended until the request can be fully considered.

7.6 Any refusal to restrict processing data should be confirmed in writing to the data subject, setting out the grounds of refusal.

Signature on behalf of Southern Projects Ltd

Signature: 
Name: Mr Gavin Nicolas Spurway
Position: Managing Director
Date: 6th of October 2025
Review Date: 6th of October 2026

The review period is a maximum of not more than 12 months

MEMORANDUM TO EMPLOYEES AND WORKERS

On 25th May 2018 the General Data Protection Regulation (GDPR) comes into force in the UK – this will be done by the Data Protection Act 2018.

The GDPR is an update to the law on data protection, with which all employers must comply.

The GDPR makes changes to an individual's rights in respect of data protection and what steps an organisation must take to ensure personal data is protected. In particular:

1. The reasons for which personal data can be processed
2. An individual's rights of access to personal data and to object to personal data being processed
3. An individual's right to ask for their personal data to be deleted
4. An organisation's responsibility to keep data secure and confidential
5. An organisation's responsibility to demonstrate compliance with data protection laws

We have set out the rights of employees in a new Data Protection Privacy Notice – Employee Information, which now forms part of our Employee Handbook and is available on request.

In addition, all employees and workers who have access to personal data in the course of their employment have individual duties to ensure that the Company complies with its obligations under the GDPR.

Therefore, we have implemented a new Data Protection Policy and Information Security Procedure which all employees and workers are required to comply with. These are also available in the Employee Handbook and will be issued to those individuals who have data protection responsibilities as part of their role.

Some employees who have access to important or sensitive personal information may be required to enter into confidentiality agreements.

If you have any questions please read the policies mentioned above first for further information, any subsequent questions should be directed to the Management.

Signature on behalf of Southern Projects Ltd

Signature: 
Name: Mr Gavin Nicolas Spurway
Position: Managing Director
Date: 6th of October 2025
Review Date: 6th of October 2026

The review period is a maximum of not more than 12 months

MEMORANDUM TO ALL SUBCONTRACTORS

On 25th May 2018 the General Data Protection Regulation (GDPR) comes into force in the UK – this will be done by the Data Protection Act 2018.

The GDPR is an update to the law on data protection, with which all employers must comply.

The GDPR makes changes to an individual's rights in respect of data protection and what steps an organisation must take to ensure personal data is protected. In particular:

1. The reasons for which personal data can be processed
2. An individual's rights of access to personal data and to object to personal data being processed
3. An individual's right to ask for their personal data to be deleted
4. An organisation's responsibility to keep data secure and confidential
5. An organisation's responsibility to demonstrate compliance with data protection laws

We have set out the rights of employees in a new Data Protection Privacy Notice – Subcontractor Information, which is always available on request.

In addition, any subcontractor who has access to personal data whilst providing Services to the Company has individual duties to ensure that the Company complies with its obligations under the GDPR.

Therefore, we have implemented a new Data Protection Policy and Information Security Procedure which all subcontractor operatives are required to comply with. These will be issued to those subcontractor operatives who have access to personal data.

Some employees who have access to important or sensitive personal information may be required to enter into confidentiality agreements.

If you have any questions please read the policies mentioned above first for further information, any subsequent questions should be directed to the Management

Signature on behalf of Southern Projects Ltd

Signature: 
Name: Mr Gavin Nicolas Spurway
Position: Managing Director
Date: 6th of October 2025
Review Date: 6th of October 2026

The review period is a maximum of not more than 12 months.