Spatial Initiative Limited (the Company): Data Protection Policy

1 Interpretation

1.1 The terms in the left hand column of the following table have the meaning in the corresponding right hand column:

Consent	a freely given, specific, informed and unambiguous indication (by way of statement or clear positive action) of the Data Subject's agreement to the Processing of Personal Data relating to them.
Data Protection Legislation	(i) unless and until the GDPR is no longer directly applicable in the UK, the General Data Protection Regulation (GDPR) and any national implementing laws, regulations and secondary legislation as amended or updated from time to time in the UK and then (ii) any successor legislation to the GDPR or the Data Protection Act 1998.
Data Protection Impact Assessment (DPIA)	a process for the purposes of identifying and minimising data protection risks.
Data Protection Manager (DPM)	the person with responsibility for data protection compliance for the Company (or their delegate from time to time).
Data Subject	a living, identified or identifiable individual about whom the Company holds Personal Data.
Data Subject Request	a request by a Data Subject to enforce rights listed in paragraph 14 of this Data Protection Policy.
EEA	the countries included in the European Economic Area from time to time.
Group	the Company and the Group Companies.
Group Companies	such companies which from time to time are a subsidiary or holding company of the Company or a subsidiary of a holding company of the Company.
Information Commissioner's Office (ICO)	the regulatory body in the UK for data protection issues

Personal Data	any information identifying a Data Subject or information relating to a Data Subject that the Company can identify (directly or indirectly) from that data alone or in combination with other identifiers which the Company possesses or can reasonably access. Personal Data includes Sensitive Personal Data. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.
Personal Data Breach	any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that the Company or its third-party service providers put in place to protect it. The accidental or unlawful destruction, loss, alteration, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.
Personal Data Processing Record	the full and accurate record maintained by the DPM on the Company's behalf of Personal Data Processing.
Personnel	all employees, workers, contractors, agency workers, consultants, directors, managers, members and others who deal with Personal Data in the context of the Company's business.
Privacy Policies	this Data Protection Policy, the Company's Data Retention Policy, Information Security Policy and Information Security Incident and Personal Data Breach Management Process
Privacy Notices	separate notices setting out information that may be provided to Data Subjects when the Company collects information about them.
Process or Processing or Processed	any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.
Sensitive Personal Data	information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

2 About this Policy

2.1 This Data Protection Policy sets out how the Company – reference to which includes all subsidiary companies - handles the Personal Data of its Personnel, customers, contacts and other third parties and should be read in conjunction with the Company's Privacy Policies. References to the Company shall be read as the relevant Company in the Group as the context requires.

2.2 This Data Protection Policy applies to all Personnel. All Personnel must read, understand and comply with this Data Protection Policy and the Company's Privacy Policies when Processing Personal Data on the Company's behalf and attend training provided on its requirements.

2.3 Any breach of this Data Protection Policy or any other Privacy Policy may result in

disciplinary action.

2.4 This Data Protection Policy does not form part of any contract between the Company and Personnel or the Company and any other third party (including clients, customers, referrers, intermediaries and agents).

3 Personal Data Protection Principles

3.1 The Company will adhere to the principles relating to Processing of Personal Data set out in the Data Protection Legislation which require Personal Data to be:

3.1.1 Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

3.1.1 collected only for specified, explicit and legitimate purposes (Purpose Limitation);

3.1.2 adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);

3.1.3 accurate and where necessary kept up to date (Accuracy);

3.1.4 not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Data Retention);

3.1.5 Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Data Security);

3.1.6 not transferred to another country without appropriate safeguards being in place (Cross Border Transfer Limitation);

3.1.7 made available to Data Subjects. In addition, Data Subjects must be allowed to exercise certain rights in relation to their Personal Data (Data Subject Requests).

3.2 The Company is responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

4 Lawfulness, Fairness and Transparency

4.1 Personal Data must be Processed lawfully, fairly and in a transparent manner.

4.2 Personnel may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. Data Protection Legislation restricts the Company's Processing of Personal Data unless there is a lawful basis for such Processing.

4.3 Lawful bases for Processing include:

4.3.1 the Data Subject has given his or her Consent;

4.3.2 the Processing is necessary for the performance of a contract with the Data Subject;

4.3.3 the Processing is necessary to meet the Company's legal obligations;

4.3.4 the Processing is necessary to protect the Data Subject's vital interests;

4.3.5 the Processing is necessary to pursue the legitimate interests of the Company or third parties provided such interests are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. Where the Company Processes Personal Data based on a legitimate interests basis, the legitimate interests must be set out in appropriate Privacy Notices.

4.4 Where the Company proposes to Process Sensitive Personal Data, additional safeguards must be considered and additional conditions may need to be satisfied. Personnel should not retain Sensitive Personal Data about other Personnel (or other individuals) on their local PC or in other areas on the Company's systems that are easily accessed; this includes keeping copies of sent emails. Sensitive Personal Data relating to Personnel should only be stored by the HR department.

4.5 Emails and records containing Sensitive Personal Data should be password protected and, if they are being shared outside of the Company, encrypted if possible. Personnel should consult with, and seek approval from, the DPM prior commencing any new activity which involves substantial Processing of any Sensitive Personal Data.

4.6 The Company must identify and document in its Personal Data Processing Record the legal basis being relied on for each Processing activity. It is the responsibility of Personnel to notify the DPM of any processing for which they have responsibility. It is the responsibility of the DPM to record the Processing in the Company's Personal Data Processing Record.

4.7 The Data Protection Legislation requires the Company to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible and in clear and plain language so that a Data Subject can easily understand them.

5 Purpose Limitation

5.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

5.2 Personnel cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless the Company has informed the Data Subject of the new purposes (and the Data Subject Consented, where necessary).

6 Data Minimisation and Accuracy

6.1 Personal Data must be adequate, relevant and limited to what is necessary for the purposes for which it is Processed. Personnel may only collect and Process Personal Data required for the purposes of job duties and should not collect excessive data.

6.2 Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate. Personnel must take all reasonable steps to ensure that the Personal Data the Company uses and holds is accurate, complete, kept up to date and relevant to the purpose for which it was

collected.

6.3 Personnel must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards in accordance with the Company's Data Retention Policy. Personnel must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

7 Data Retention

7.1 Personal Data must not be kept in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which it was originally collected, including for the purpose of satisfying any legal, accounting or reporting requirements.

7.2 Personnel must comply with the Company's Data Retention Policy from time to time which recommends the maximum periods for which Personal Data should normally be retained.

7.3 Personnel will take all reasonable steps to destroy or erase from the Company's systems all Personal Data that the Company no longer requires in accordance with the Company's Data Retention Policy. Personnel should seek the assistance of the Company's IT Department as is appropriate. Personnel should also consider requiring third parties to delete Personal Data where appropriate.

7.4 The Company will ensure Data Subjects are informed of the period for which Personal Data is stored in any applicable Privacy Notice.

8 Data Security

8.1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing and against accidental loss, destruction or damage.

8.2 The Company has developed and implemented and will continue to develop and maintain safeguards appropriate to its size, scope and business. The Company will regularly evaluate and test the effectiveness of those safeguards to ensure security of its Processing of Personal Data.

8.3 Personnel are also responsible for protecting the Personal Data the Company holds. Personnel must Process Personal Data in accordance with the Company's policies, instructions and guidance from time to time (including the Company's Information Security Policy). Personnel must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

8.4 Personnel may only transfer Personal Data to third-party service providers who agree to comply with such policies and procedures as the Company requires and which agree to put adequate measures in place.

8.5 Personnel must comply with all instructions in relation to the administrative, physical and technical safeguards or applications the Company maintains to protect Personal Data and must not attempt to circumvent any of them. Failure to comply with such instructions will be dealt with in accordance with the Company's Disciplinary Policy and may result in dismissal.

9 Reporting a Personal Data Breach

9.1 The Data Protection Legislation requires the Company to notify certain Personal Data Breaches to the Information Commissioner's Office (**ICO**) and, in some instances, the Data Subject. Notification is required within 72 hours.

9.2 Where a Personal Data Breach has occurred or is suspected, Personnel should not attempt to respond to the incident alone but should immediately notify their line manager or, in the line manager's absence, the DPM, who will manage the data breach in accordance with the Company's Information Security Incident and Personal Data Breach Process. Personnel should preserve all evidence relating to any Personal Data Breach or potential Data Breach.

10 Cross Border Transfer Limitation

10.1 The Data Protection Legislation restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to Data Subjects by the Data Protection Legislation is not undermined. Personal Data is transferred across borders when it is transmitted or sent from the country in which it originates to a different country or when it is viewed or accessed from a different country.

10.2 Personnel may only transfer Personal Data outside the EEA where the written authority of the DPM has first been given.

11 Automated Decision-Making

11.1 Automated decision-making is generally prohibited when a decision has a legal or similar significant effect on a Data Subject. If a decision is to be based solely on automated Processing, then Personnel must consult with the DPM and follow any guidance issued by the DPM.

12 Direct Marketing

12.1 The Company is subject to certain rules and privacy laws when marketing to its customers. Personnel must not engage in direct marketing which is without the authority of the Marketing Department and must follow the Company's Direct Marketing Policy and any guidance issued by the DPM in connection with any initiative in relation to direct marketing.

12.2 Personnel must not maintain marketing lists or marketing databases on local PCs or personal areas of the network. Marketing lists and databases are held centrally by the Marketing Department.

12.3 A Data Subject's objection to direct marketing must be promptly honoured.

13 Data Subject's Requests

13.1 A Data Subject Request is a request made by or on behalf of a Data Subject to enforce their rights pursuant to Data Protection Legislation.

13.2 In certain circumstances and subject to limitations, Data Subjects have the right to:

13.2.1 **Request access to Personal Data** (commonly known as a "data subject

access request"). This enables Data Subjects to receive a copy of the Personal Data the Company holds about them and to check that the Company is lawfully Processing it.

13.2.2 **Request correction of the Personal Data.** This enables Data Subjects to have any incomplete or inaccurate Personal Data the Company holds about them corrected.

13.2.3 **Request erasure of Personal Data**. This enables Data Subjects to ask the Company to delete or remove Personal Data where there is no good reason for the Company continuing to Process it.

13.2.4 **Object to processing of Personal Data.** Where the Company is relying on a legitimate interest (or that of a third party) as a lawful basis for Processing and there is something about a particular situation which makes the Data Subject want to object to Processing on this ground.

13.2.5 **Request the restriction of Processing of Personal Data**. This enables Data Subjects to ask the Company to suspend the Processing of Personal Data about them, for example, if the Data Subject wants the Company to establish its accuracy or the reason for Processing it.

13.2.6 **Request the transfer** of certain categories of Personal Data to another party.

13.3 If Data Subjects wish to exercise the above rights in relation to Personal Data they should submit their request, normally in writing, to the DPM using the contact details at the end of this Policy. Only Personnel authorised by the DPM shall respond to Data Subject Requests.

13.4 Data Subject Requests must receive a prompt response and be issued no later than **one month** after the date on which the request is received. This can be extended in limited circumstances as advised by the DPM.

13.5 The Company shall not charge a fee when responding to a Data Subject Request, unless the request is unfounded or excessive. In such instances, the Company may charge a reasonable fee that takes into account the administrative costs of taking the necessary action to respond. Where request is unfounded or unreasonable, the Company may also refuse to act on the request.

13.6 In limited circumstances, the Company may be exempt from complying (in whole or in part) with the Data Subject Request. Exemptions may apply, for example, for reasons relating to the public interest, the prevention of crime or for reasons relating to legal proceedings.

13.7 The Company is required to respond to a Data Subject Request in relation to Personal Data held at the time the request was received. Under no circumstances should Personnel amend or delete Personal Data other than in the ordinary course of business once a Data Subject Request has been received.

14 Role of the DPM

14.1 Personnel must always contact the DPM for advice and guidance in the following circumstances:

14.1.1 where there is uncertainty about the lawful basis which the Company is relying on to process Personal Data (including the legitimate interests used by the Company) see section 4.3.

14.1.2 where there is a need to rely on Consent (see section 4.3);

14.1.3 where there is a need to draft Privacy Notices (see section 4.7);

14.1.4 where there is uncertainty about the retention period for the Personal Data being Processed (see section 7);

14.1.5 where there is uncertainty about what security or other measures Personnel need to observe to protect Personal Data (see section 8);

14.1.6 where there has been a Personal Data Breach (see section 9);

14.1.7 where there is uncertainty about on what basis to transfer Personal Data outside the EEA (see section 10);

14.1.8 on receipt of a Data Subject Request (see section 13);

14.1.9 where a significant new, or change in, Processing activity which may require a DPIA (see section 15) or there is a proposal to use Personal Data for purposes incompatible with those it was collected for;

14.1.10 where there is a proposal to undertake any activities involving automated decision-making (see section 11);

14.1.11 where there is a proposal to carry out direct marketing activities (see section 12); or

14.1.12 where there is a proposal to share Personal Data with third parties (see section 15).

15 Accountability

Record Keeping

15.1 The Company keeps full and accurate records of all its data Processing activities (Personal Data Processing Record).

15.2 Personnel must assist the Company in keeping and maintaining an accurate Personal Data Processing Record reflecting the Company's Processing.

15.3 In relation to Data Processing under their control, Personnel must provide the DPM with requested details including: clear descriptions of the types of Personal Data, categories of Data Subjects, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, Personal Data retention periods and a description of the security measures in place.

Privacy by Design and Data Protection Impact Assessment

15.4 The Company is required to implement appropriate and effective technical and organisational measures when Processing Personal Data to ensure compliance with data privacy principles.

15.5 Personnel must assess what measures can be implemented in relation to all systems and processes in their area of responsibility which Process Personal Data by taking into account the nature, scope, context and purposes of Processing, the risks of likelihood and severity of harm to Data Subject's rights posed by the Processing, the state of the art and the cost of implementation.

15.6 A formal Data Protection Impact Assessment (DPIA) is mandatory where proposed Processing is likely to result in a high risk of harm to Data Subject's rights either because there is a high probability of some harm or a lower possibility of serious harm. High risks are likely to arise where Processing involves, for example, use of new technologies, largescale Processing (particularly of Sensitive Personal Data), profiling and tracking Data Subject's location or behaviours, automated decision making or combining or matching data from multiple sources.

15.7 Where a DPIA is required, this must be prepared, discussed with and approved by the DPM. A DPIA must include:

15.7.1 a description of the Processing, its purposes and the legitimate interests relied on, if appropriate;

15.7.2 an assessment of the necessity and proportionality of the Processing in relation to its purpose;

15.7.3 an assessment of the risk to Data Subjects; and

15.7.4 the risk mitigation measures in place and demonstration of compliance.

Sharing Personal Data

15.8 Generally, the Company is not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

15.9 Personnel may only share the Personal Data the Company holds with another employee, agent or representative of the Company if the recipient has a job-related need to know the information.

15.10 Personnel may only share the Personal Data the Company holds with third parties, such as the Company service providers, if:

15.10.1 they have a need to know the information for the purposes of providing the contracted services;

15.10.2 sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

15.10.3 the third party has agreed to comply with any required data security standards, policies and procedures and put adequate security measures in place;

15.10.4 the transfer complies with any applicable cross border transfer restrictions; and

15.10.5 a fully executed written contract that contains approved third party clauses has been obtained.

Training and Audit

15.11 Personnel must undergo all mandatory data privacy related training and ensure that their reports undergo similar mandatory training.

15.12 Personnel must regularly review all the systems and processes under their control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

16 Changes to this Data Protection Policy

16.1 The Company reserves the right to change this Data Protection Policy at any time without notice. It is the responsibility of Personnel to ensure that their knowledge of this Data Protection Policy is up to date and that they comply with its terms.