Abbey Scaffolding (Swindon) Ltd

Data Protection Policy

Updated 22/9/2022

1. **Introduction**

This Policy sets out the obligations of Abbey Scaffolding (Swindon) Ltd, a company registered in England under 03788384, whose registered office is at Unit 30 + 31 Whitehill Industrial Park, Royal Wootton Bassett, Swindon, Wiltshire, SN4 7DB (“the Company”) regarding data protection and the rights of employees, customers, business contacts and suppliers (“data subjects”) in respect of their personal data under The Data Protection Act 2018 (DPA)

The DPA defines “personal data” as any information relating to an identified or identifiable natural person (a “data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets the Company’s obligations regarding the collection, processing, transfer, storage and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

1. **The Data Protection Principles**

This policy aims to ensure compliance with the DPA and sets out the following principles with which any party handling personal data must comply. All personal data must be:

* 1. Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
  2. Collected for specified, explicit, and legitimate purposes and not further process in a manner that is incompatible with those purposes.
  3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
  4. Accurate and kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, is erased or rectified without delay.
  5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes.
  6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

1. **The Rights of Data Subjects**

The DPA sets out the following rights applicable to data subjects:

* 1. The right to be informed
  2. The right of access
  3. The right to rectification
  4. The right to erasure (also known as the ‘right to be forgotten’)
  5. The right to restrict processing
  6. The right to data portability
  7. The right to object
  8. Rights with respect to automated decision-making and profiling

1. **Lawful, Fair, and Transparent Data Processing**
   1. The DPA seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The DPA states that processing of personal data shall be lawful if at least one of the following applies.
      1. The data subject has given consent to the processing of their personal data for one or more specific purposes;
      2. The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;
      3. The processing is necessary for compliance with a legal obligation to which the data controller is subject;
      4. The processing is necessary to protect the vital interests of the data subject or of another natural person;
      5. The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
      6. The processing is necessary for the purposes of the legitimate interest pursued by the data controller or by the third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
2. **Specified, Explicit, and Legitimate Purposes**
   1. The Company collects and processes the personal data. This includes:
      1. Personal data collected directly from data subjects
   2. The Company only collects, processes, and holds personal data for the specific purposes.
   3. Data subjects are kept informed at all times of the purpose for which the Company uses their personal data.
3. **Adequate, Relevant, and Limited Data Processing**

The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed)

1. **Accuracy of Data and Keeping Data Up-to-Date**
   1. The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject.
   2. The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase the data, as appropriate.
2. **Data Retention**
   1. The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held and processed.
   2. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.
3. **Secure Processing**

The Company shall ensure that all personal data collected, held and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

1. **Accountability and Record-Keeping**
   1. The Company’s Data Protection Officer is James Barnett, contact details are Tel: 01793 480347, email: [office@abbeyscaffold.com](mailto:office@abbeyscaffold.com)
   2. The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company’s other data protection-related policies, and with the DPA and other applicable data protection legislation.
   3. The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:
      1. The Name and details of the Company, its Data Protection Officer, and any applicable third-party data processors;
      2. The purposes for which the Company collects, holds, and processes personal data;
      3. Details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates;
      4. Details of how long personal data will be retained by the Company
      5. Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.
2. **Keeping Data Subjects Informed**
   * 1. Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collections; and
     2. Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
3. If the personal data is used to communicate with the data subject, when the first communication is made; or
4. If the personal data is to be transferred to another party, before that transfer is made; or
5. As soon as reasonable possible and in any event not more than one month after the personal data is obtained.
   1. The following information shall be provided:
      1. Details of the Company including, but not limited to, the identity of its Data Protection Officer;
      2. The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;
      3. Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of personal data;
      4. Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
      5. Where the personal data is to be transferred to one or more third parties, details of those parties;
      6. Details of data retention;
      7. Details of the data subject’s rights under the DPA;
      8. Details of the data subject’s right to withdraw their consent to the Company’s processing of their personal data at any time;
      9. Details of the data subject’s right to complain to the Information Commissioner’s Office (the “supervisory authority” under the DPA);
      10. Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;
      11. Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.
6. **Data Subjects Access**
   1. Data subjects may make Subject Access Requests (SARs”) at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.
   2. Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to the Company’s Data Protection Officer at [office@abbeyscaffold.com](mailto:office@abbeyscaffold.com).
   3. Responses to SAR’s shall normally be made within one week of receipt, however this may be extended by up to one month if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.
   4. All SAR’s received shall be handled by the Company’s Data Protection Officer.
   5. The Company does not charge a fee for the handling of normal SAR’s.
7. **Rectification of Personal Data**
   1. Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.
   2. The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue.
   3. In the event that any affected personal data has been disclosed to third parties, those third parties shall be informed of any rectification that must be made to that personal data.
8. **Erasure of Personal Data**
   1. Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:
      1. It is no longer necessary for the Company to hold that personal data with respect to purpose(s) for which it was originally collected or processed;
      2. The data subject wishes to withdraw their consent to the Company holding and processing their personal data;
      3. The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (See Part 18 of this Policy for further details concerning the right to object);
      4. The personal data has been processed unlawfully;
      5. The personal data needs to be erased in order for the Company to comply with a particular legal obligation
      6. The personal data is being held and processed for the purpose of providing information society services to a child.
   2. Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject’s request.
   3. In the event that any personal data that is to be erased in response to a data subject’s request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).
9. **Restriction of Personal Data Processing**
   1. Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.
   2. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).
10. **Objections to Personal Data Processing**
    1. Data subjects have the right to object to the Company processing their personal data based on legitimate interests, direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.
    2. Where a data subject objects to the Company processing their personal data based on it legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company’s legitimate grounds for such processing override the data subject’s interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.
    3. Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.
    4. Where a data subject objects to the company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under DPA, “demonstrate grounds relating to his or her particular situation”. The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.
11. **Data Security – Transferring Personal Data and Communications**

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

* 1. All emails containing personal data must be encrypted
  2. Transmission over unsecured networks is not permitted in any circumstances;
  3. Personal data may be not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
  4. Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted.
  5. Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient

1. **Data Security – Storage**

The Company shall ensure that the following measures are taken with respect to the storage of personal data:

* 1. All electronic copies of personal data should be stored securely using passwords;
  2. All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;
  3. All personal data stored electronically should be backed up weekly with backups stored offsite. All backups should be encrypted;
  4. No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise without formal written approval of James Barnett and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time approval is given, and for no longer than is absolutely necessary.
  5. No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with this Policy and the DPA.

1. **Data Security – Disposal**

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

1. **Data Security – Use of Personal Data**

The Company shall ensure that the following measures are taken with respect to the use of personal data:

* 1. No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from James Barnett.
  2. No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of James Barnett.
  3. Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;
  4. If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it

1. **Data Security – IT Security**

The Company shall ensure that the following measures are taken with respect to IT and information security:

* 1. All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers and symbols. All software used by the Company is designed to require such passwords.
  2. Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
  3. All software (including, but no limited to, applications and operating systems) shall be kept up-to-date. The Company’s IT staff shall be responsible for installing any all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so; and
  4. No software may be installed on any Company-owned computer or device without prior approval of the Company director.

1. **Organisational Measures**

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data;

* 1. All employees, agents, sub-contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company’s responsibilities under the DPA and under this Policy, and shall be provided with a copy of this Policy;
  2. Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;
  3. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
  4. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;
  5. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encourage to exercise care, caution, and

discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

* 1. Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
  2. All personal data held by the Company shall be reviewed periodically,
  3. The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
  4. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the DPA and this Policy by contract;
  5. All agents, contactors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the DPA; and
  6. Where any agent, contractor, or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

1. **Data Breach Notification**
   1. All personal data breaches must be reported immediately to the Company’s Data Protection Officer.
   2. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner’s Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
   3. In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.
   4. Data breach notifications shall include the following information:
      1. The categories and approximate number of data subjects concerned;
      2. The categories and approximate number of personal data records concerned;
      3. The name and contact details of the Company’s Date Protection Officer (or other contact point where more information can be obtained);
      4. The likely consequences of the breach;
      5. Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measure to mitigate its possible adverse effects.

This Policy has been approved and authorised by:

**Name: Mr James Barnett**

**Position: Managing Director**

**Date: Sept 2022**

**Due for Review by: Jan 2023**

**Signature:** 