PRIVACY STATEMENT FOR PLEDGE OFFICE CHAIRS LTD

1. INTRODUCTION

1.1 The Pledge Office Chairs Ltd (the "Company") places high importance on the correct, lawful, and fair handling of all Personal Data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

1.2 The purpose of this policy is to ensure that the Company carries out its business in accordance with applicable personal data protection regulations, including the General Data Protection Regulation ("GDPR") so that everyone's fundamental right to data protection is duly preserved, guaranteed and respected.

1.3 The Company has appointed Beverley Pledger as the person with responsibility for data protection compliance within the organisation. She can be contacted at privacy@pledgechairs.co.uk. Questions about this policy, or requests for further information, should be directed to her.

1.4 It is the responsibility of every manager to ensure that their team members are aware of and comply with the obligations under the rules set out in this policy and to organise the training necessary for them to comply with the requirements of this policy.

2. SCOPE

2.1 This policy applies to all Staff of the Company together with contractors, consultants and agency Staff who are subject to the conditions and scope of this policy. If you collect, store and/or process personal data or supervise staff involved in these activities you must ensure that you follow the requirements of this policy at all times.

2.2 The policy applies to all Processing of Personal Data.

3. DEFINITIONS

3.1 Controller: Pledge Office Chairs Ltd registered at Mill Road, Leighton Buzzard, Bedfordshire, LU7 1BA. We trade as Pledge Office Chairs Ltd.

3.2 Data Access Request (SAR): A formal request to the Company from a Data Subject to access their Personal Data. This should be in writing.

3.3 Data Subject: The individual to whom the Personal Data relates.

3.4 Direct Marketing: Any communication by whatever means of any advertising or marketing material that is directed to particular individuals. This will include any materials sent by mail, electronic communications, telephone or fax.

3.5 External Data Processors: Third party organisations or individuals that are contracted to provide the Company with Personal Data processing. These can include:

3.5.1 Payroll and management of employees.

3.5.2 Data archiving/destruction.

3.5.3 Website hosting services.

3.5.4 Data screening, mailing house services and other marketing support services.

3.5.5 Courier and despatch services.

3.5.6 Confidential waste destruction.

3.5.7 Business or operational administration.

3.5.8 Agents, contractors, consultants or other parties working on behalf of the Company.

3.5.9 Any outsourcing activity.

3.6 Personal Data: 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 such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. It also includes opinions about individuals as well as facts and also applies to corporate contacts.

Personal Data includes data held electronically on a computer or network and data held in hard copy paper format including, for example, on microfiche, hand held devices, mobiles, laptops, databases and filing cabinets.

3.7 Processing: This is a wide-ranging term that, in practice, covers any use of Personal Data including:

3.7.1 Obtaining, recording, holding, and carrying out any operation(s) on the Personal Data.

3.7.2 Organisation or alteration of the Personal Data.

3.7.3 Retrieval, disclosure or use of the Personal Data.

3.7.4 All such data processing activities will constitute Processing within the meaning of data protection laws.

3.8 Sensitive Personal Data: Any information about or pertaining to an individual's physical or mental health, racial or ethnic origin, sexual life, politics, religion, trade union membership, or any information about alleged or committed criminal offences.

3.9 Staff: Any current or former job applicant, employee, apprentice, intern, volunteer, or casual worker of the Company.

4. DATA PROTECTION PRINCIPLES

4.1 This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling Personal Data must comply. All Personal Data must be:

4.1.1 processed lawfully, fairly, and in a transparent manner in relation to the Data Subject (Principle of Lawfulness);

4.1.2 collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes (Principle of Specified Purpose);

4.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Principle of Concision);

4.1.4 accurate and kept up to date having regard to the purposes for which they are processed, is erased or rectified without delay (Principle of Accuracy);

4.1.5 kept in a form which permits identification of the Data Subject for no longer than is necessary for the purposes for which the Personal Data is processed (Principle of Temporariness); and

4.1.6 processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against the loss, destruction or accidental damage thereof, by means of the application of appropriate technical or organisational measures (Principle of Integrity and Confidentiality).

5. PRINCIPLE OF LAWFULNESS

5.1 The GDPR seeks to ensure that Personal Data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the Data Subjects. The Company must have a "lawful" reason for collecting data, i.e. at least one of the following reasons:

5.1.1 consent is given by the Data Subject to the processing of his or her Personal Data for one or more specific purposes;

5.1.2 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;

5.1.3 for compliance with a legal obligation to which the Controller is subject;

5.1.4 to protect the vital interests of the Data Subject or of another natural person;

5.1.5 for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller; and

5.1.6 for the purposes of the legitimate interests pursued by the Controller or by a 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.

6. Staff must not Process or store Sensitive Personal Data unless this is necessary and then only if the Data Subject has explicitly consented. A record of that consent must be retained as required by the Company.

7. PRINCIPLE OF SPECIFIED PURPOSE

7.1 The Company collects, and processes Personal Data set out in Part 13 of this Policy.

7.2 The Company only processes Personal Data for the specific purposes set out in Part 13 of this Policy.

7.3 The purposes for which the Company processes Personal Data will be informed to Data Subjects at the time that their Personal Data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

7.4 Any Personal Data collected for a specific purpose may not be subsequently processed for a different purpose. Should it prove necessary to radically change the purpose for which the Personal Data in question were collected, Staff will be required to inform the Data Subjects of the change in question beforehand.

8. PRINCIPLE OF CONCISION

8.1 This Company shall ensure the Processing of Personal Data is adequate, relevant and not excessive for the specific purposes for which the data was obtained. The most appropriate time for informing the Data Subject with notice of the purposes of collection is at the time the Personal Data is collected.

9. PRINCIPLE OF CONCISION

9.1 The Company shall ensure that all Personal Data collected and processed is kept secure and protected against unauthorised or unlawful Processing and against accidental loss, destruction or damage.

10. PRINCIPLE OF ACCURACY

10.1 The Company shall ensure that all Personal Data collected and processed is kept accurate and up-to-date and it must be relevant and not excessive.

10.2 The accuracy of data shall be checked when it is collected and at periodic intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken to amend or erase that data, as appropriate

11. PRINCIPLE OF TEMPORARINESS

11.1 The Company shall not keep Personal Data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it safely without delay. Staff must abide by the Company's data retention practices.

12. PRINCIPLE OF INTEGRITY AND CONFIDENTIALITY.

12.1 The Company shall take sufficient technical and organisational measures to ensure that Personal Data is kept secure. This includes the physical security of the hardware and software, staff awareness and training and the development of adequate polices and processes.

13. PERSONAL DATA

13.1 The following personal data may be collected, held, and processed by the Company:

13.1.1 Contact details for existing and prospective customers and suppliers, associated with the production, sale and after sales service of office seating solutions.

13.1.2 for Staff as stated in the applicable privacy notice issued to you by the Company; and for

14. ACCOUNTABILITY

14.1 The Company shall keep written internal records of all Personal Data Processing, which shall incorporate the following information:

14.1.1 the name and details of the Company and any applicable third-party data controllers;

14.1.2 the purposes for which the Company processes Personal Data;

14.1.3 details of the categories of Personal Data collected, held, and processed by the Company; and the categories of Data Subjects to which that Personal Data relates;

14.1.4 details (and categories) of any External Data Processors that will receive Personal Data from the Company;

14.1.5 details of any transfers of Personal Data to non-EEA countries including all mechanisms and security safeguards;

14.1.6 details of how long Personal Data will be retained by the Company; and

14.1.7 detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of Personal Data.

15. PRIVACY IMPACT ASSESSMENTS

15.1 The Company shall carry out Privacy Impact Assessments when and as required under GDPR and it shall address the following areas of importance:

15.1.1 the purpose(s) for which Personal Data is being processed and the Processing operations to be carried out on that data;

15.1.2 details of the legitimate interests being pursued by the Company;

15.1.3 an assessment of the necessity and proportionality of the Processing with respect to the purpose(s) for which the data is being processed;

15.1.4 an assessment of the risks posed to individual Data Subject; and

15.1.5 details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of Personal Data, sufficient to demonstrate compliance with the GDPR.

16. THE RIGHTS OF DATA SUBJECTS

16.1 The Company must ensure the rights of Data Subjects must be observed and Staff must take all reasonable steps to ensure that they are aware of and respect these rights. These rights include:

16.1.1 the right to be informed, please see point 16;

16.1.2 the right of access, please see point 17;

16.1.3 the right to rectification;

16.1.4 the right to erasure (also known as the 'right to be forgotten');

16.1.5 the right to restrict processing;

16.1.6 the right to data portability;

16.1.7 the right to object; and

16.1.8 rights with respect to automated decision-making and profiling.

17. KEEPING DATA SUBJECTS INFORMED

17.1 Any data gathered from the Company's website will be subject to consent via our Privacy Notice. For all other Data Subjects when Personal Data is collected they will be provided with at least the following information:

17.1.1 details of the Company;

17.1.2 the purpose(s) for which the Personal Data is being collected and will be processed;

17.1.3 If applicable, the legitimate interests upon which the Company is justifying its collection and processing of the Personal Data;

17.1.4 where the Personal Data is not obtained directly from the Data Subject, the categories of Personal Data collected and processed;

17.1.5 where the Personal Data is to be transferred to one or more third parties, details of those parties for example IT and payroll providers;

17.1.6 details of the length of time the Personal Data will be held by the Company (or, where there is no predetermined period, details of how that length of time will be determined);

17.1.7 details of the Data Subject's rights under the GDPR;

17.2 where applicable, any countries not belonging to the European Economic Area or Switzerland to which the Company or its subsidiaries intend to transfer the Personal Data, and the level of protection offered by said countries;

17.2.1 reference to the Data Subject's Request Response Procedure setting out Data Subject's right to withdraw their consent to the processing of Personal Data, make a subject access, to complain to the Information Commissioner's Office; and

17.2.2 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.

18. DATA SUBJECT ACCESS

18.1 A Data Subject may make a subject access request ("SAR") at any time to find out more about the Personal Data which the Company holds about them. The Company is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests and in such cases the Data Subject shall be informed of the need for the extension).

18.2 The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a Data Subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

18.3 For full details please the Company's Subject Access Request Procedure which also includes reference to the following:

18.3.1 Rectification.

18.3.2 Erasure.

18.3.3 Restrictions.

18.3.4 Objections.

18.3.5 A Data Access Request may be received in any number of forms, including a telephone call, email or letter. In the case of a telephone call, the Data Subject should be requested to submit the Data Access Request in writing to the Beverley Pledger. In some cases, the Company may need to ask for proof of identification before the request can be processed. The Company will inform the individual if it needs to verify his/her identity and the documents it requires. Beverley Pledger should be notified of the request and of the response.

18.4 The Company will make reasonable adjustments as appropriate for disabled people who make a SAR e.g. it will respond in a particular format that is accessible to the disabled person, such as Braille, large print, email, or audio formats.

18.5 Any Staff receiving a Data Access Request must immediately forward it to the Beverley Pledger.

18.6 Under no circumstances should unauthorised Staff respond to a Data Access Request. Data access requests will be responded to by a Director.

19. DATA PROTECTION MEASURES

19.1 The Company shall ensure that all its Staff, agents, contractors, or other parties working on its behalf comply with the following when working with Personal Data:

19.1.1 all emails containing Personal Data must be encrypted;

19.1.2 where 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. Hardcopies should be shredded, and electronic copies should be deleted securely;

19.1.3 Personal Data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

19.1.4 where Personal Data is to be sent by facsimile transmission the recipient should be informed in advance of the forthcoming transmission;

19.1.5 where Personal Data is to be transferred in hardcopy form it should be passed directly to the recipient;

19.1.6 no Personal Data may be shared informally and if a Staff, 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 them.

19.1.7 all hardcopies of Personal Data, along with any electronic copies stored on physical, removable media should be stored securely in a locked drawer, cabinet, or office;

19.1.8 Personal Data must be handled with care at all times and should not be left unattended or on view to unauthorised Staff, agents, sub-contractors, family, or other parties including the general public at any time;

19.1.9 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;

19.1.10 no Personal Data should be transferred to any device personally belonging to

19.1.11 Staff 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 the letter and spirit of this Policy and of GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken);

19.1.12 all Personal Data stored electronically should be backed up every 24 hours with backup's stored offsite;

19.1.13 all electronic copies of Personal Data should be stored securely using passwords and data encryption;

19.1.14 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; and

19.1.15 under no circumstances should any passwords be written down or shared between any Staff, 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.

20. ORGANISATIONAL MEASURES

20.1 The Company shall ensure that the following measures are taken with respect to the Processing of Personal Data:

20.1.1 all Staff, External Data Processors and others working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under GDPR and under this Policy, and shall be provided with a copy of this Policy;

20.1.2 only Staff, External Data Processors and others 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;

20.1.3 all Staff, External Data Processors and others working on behalf of the Company handling Personal Data will be appropriately trained to do so;

20.1.4 all Staff, External Data Processors and others working on behalf of the Company handling Personal Data will be appropriately supervised;

20.1.5 methods of Processing Personal Data shall be regularly evaluated and reviewed;

20.1.6 the performance of those Staff, External Data Processors and others working on behalf of the Company handling Personal Data shall be regularly evaluated and reviewed;

20.1.7 all Staff and External Data Processors working on behalf of the Company handling Personal Data will be bound to do so in accordance with the principles of GDPR and this Policy by contract;

20.1.8 all External Data Processors and others working on behalf of the Company handling Personal Data must ensure that any and all of their employees/workers who are involved in the Processing of Personal Data are held to the same conditions as those relevant to Staff of the Company arising out of this Policy and the GDPR; and

20.1.9 where the handling of Personal Data by External Data Processors or others working on behalf of the fails short of their obligations to the Company 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.

21. DIRECT MARKETING

22. The Company shall comply with the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) regarding Direct Marketing.

23. CHILDREN

23.1 The Company recognises that the use of child data for marketing or for profiling requires specific protection. The Company shall comply with the following restrictions in respect of processing Personal Data relating to children:

23.1.1 parental consent will be obtained for Online services offered directly to children;

23.1.2 any information provided to a child in relation to their rights as a Data Subject shall be concise, transparent, intelligible and easily accessible, using clear and plain language.

24. Beverley Pledger shall be immediately informed if any of the above activities are compromised.

25. DATA BREACH NOTIFICATION

25.1 All Personal Data breaches must be reported immediately to Beverley Pledger.

25.2 If a Personal Data breach occurs and that breach is likely to result in a risk to the rights and freedoms of a Data Subject (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Beverley Pledger must notify the Managing Director and 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.

25.3 In the event that a Personal Data breach is likely to result in a high risk to the rights and freedoms of a Data Subject, Beverley Pledger must ensure that the affected Data Subject is informed of the breach directly and without undue delay.

25.4 Data breach notifications shall include the following information:

25.4.1 the categories and approximate number of Data Subjects concerned;

25.4.2 the categories and approximate number of Personal Data records concerned;

25.4.3 the name and contact details of the Company's contact point where more information can be obtained;

25.4.4 the likely consequences of the breach;

25.4.5 details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

26. REPORTING NON-COMPLIANCE

26.1 Staff who know or suspect that this policy may have been violated must immediately notify their line manager. Alternatively, if they believe that the matter is sufficiently serious, they may contact a Director [DPO].

27. CONSEQUENCES OF NON-COMPLIANCE

27.1 Staff who violate this policy are subject to disciplinary action, up to and including summary dismissal. Staff may also incur criminal liability if they knowingly or recklessly obtain and/or disclose Personal Data without the consent of the Company i.e. outside the legitimate purposes of the Company.

27.2 External Data Processors who violate the applicable parts of this policy are subject to termination of all contracts with the Company. In addition, access to the Company may be withdrawn and criminal prosecution taken.

28. CONTACTS

In the first instance all enquiries or requests for further information or guidance relating to data protection should be addressed to Beverley Pledger and or emailed to privacy@pledgechairs.co.uk