

Data Protection Policy

1. Purpose

This Policy sets out the obligations of HeadStart Speech & Behaviour Therapies, regarding data protection and the rights of staff, clients, business contacts etc. in respect of their personal data under the Data Protection Legislation (defined below).

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.

2. Definitions

“consent”	means the consent of the data subject which must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they (by a statement or by a clear affirmative action) signify their agreement to the processing of personal data relating to them;
“data controller”	means the person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, the Company is the data controller of all personal data relating to data subject, e.g. staff, customers, business contacts etc, used in our business;
“data processor”	means a person or organisation which processes personal data on behalf of a data controller;
“Data Protection Legislation”	means all applicable data protection and privacy laws including, but not limited to, the GDPR, and any applicable national laws, regulations, and secondary legislation in England and Wales concerning the processing of personal data or the privacy of electronic communications, as amended, replaced, or updated from time to time;
“data subject”	means a living, identified, or identifiable individual about whom the Company holds personal data;
“EEA”	means the European Economic Area, consisting of all EU Member States, Iceland, Liechtenstein, and Norway;

“personal data”	means any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, 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 data subject;
“personal data breach”	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed;
“processing”	means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
“pseudonymisation”	means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person; and
“special category personal data”	means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, biometric, or genetic data.

3. Data Protection Officer & Scope of Policy

- 3.1 The Company’s Data Protection Officer is Gareth Ewers-Cobb, admin@headstartaba.org, 07375064745. The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies (including those referred to in this Policy), procedures, and/or guidelines.
- 3.2 All line-managers and supervisors are responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of the Company comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.
- 3.3 Any questions relating to this Policy, the Company’s collection, processing, or holding of personal data, or to the Data Protection Legislation should be referred to the Data Protection Officer.

4. The Data Protection Principles

4

The Data Protection Legislation sets out the following principles with which any party handling personal data must comply. All personal data must be:

- 4.1 processed lawfully, fairly, and in a transparent manner in relation to the data subject;
- 4.2 collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- 4.3 adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;
- 4.4 accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay;
- 4.5 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 in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the Data Protection Legislation in order to safeguard the rights and freedoms of the data subject;
- 4.6 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.

5. The Rights of Data Subjects

The Data Protection Legislation sets out the following key rights applicable to data subjects:

- 5.1 The right to be informed;
- 5.2 the right of access;
- 5.3 the right to rectification;
- 5.4 the right to erasure (also known as the 'right to be forgotten');
- 5.5 the right to restrict processing;
- 5.6 the right to data portability;
- 5.7 the right to object; and
- 5.8 rights with respect to automated decision-making and profiling.

6. Lawful, Fair and Transparent Data Processing

- 6.1. The Data Protection Legislation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Specifically, the GDPR states that processing of personal data shall be lawful if at least one of the following applies:
- 6.1.1. the data subject has given consent to the processing of their personal data for one or more specific purposes;
 - 6.1.2. 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;
 - 6.1.3. the processing is necessary for compliance with a legal obligation to which the data controller is subject;
 - 6.1.4. the processing is necessary to protect the vital interests of the data subject or of another natural person;
 - 6.1.5. 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
 - 6.1.6. the processing is necessary for the purposes of the legitimate interests pursued by the data 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.
- 6.1 [If the personal data in question is special category personal data (also known as 'sensitive personal data'), at least one of the following conditions must be met:
- 6.1.1 the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);
 - 6.1.2 the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);
 - 6.1.3 the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
 - 6.1.4 the data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
 - 6.1.5 the processing relates to personal data which is manifestly made public by the data subject;

- 6.1.6 the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
- 6.1.7 the processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
- 6.1.8 the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;
- 6.1.9 the processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or
- 6.1.10 the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.]

7 Consent

If consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, the following shall apply:

- 7.1 Consent is a clear indication by the data subject that they agree to the processing of their personal data. Such a clear indication may take the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity are unlikely to amount to consent.
- 7.2 Where consent is given in a document which includes other matters, the section dealing with consent must be kept clearly separate from such other matters.
- 7.3 Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly.
- 7.4 If personal data is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal data was originally collected that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject.

- 7.5 [If special category personal data is processed, the Company shall normally rely on a lawful basis other than explicit consent. If explicit consent is relied upon, the data subject in question must be issued with a suitable privacy notice in order to capture their consent.]
- 7.6 In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, records must be kept of all consents obtained in order to ensure that the Company can demonstrate its compliance with consent requirements.

8 Specified, Explicit and Legitimate Purposes

8.1 The Company collects and processes the personal data set out in parent homes, schools or community settings.

8.1.1 personal data collected directly from data subjects:

OR

8.1.2 personal data obtained from third parties.

8.2 The Company only collects, processes, and holds personal data for the specific purposes set out in practice management software, or data folder left in the family home (or for other purposes expressly permitted by the Data Protection Legislation).

8.3 Data subjects must be kept informed at all times of the purpose or purposes for which the Company uses their personal data. Please refer to Part 15 for more information on keeping data subjects informed.

9 Adequate, Relevant and Limited

9.1 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) as under Part 8, above, and as set out in client practice management software, data folder.

9.2 Employees, agents, contractors, or other parties working on behalf of the Company may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected.

9.3 Employees, agents, contractors, or other parties working on behalf of the Company may process personal data only when the performance of their job duties requires it. Personal data held by the Company cannot be processed for any unrelated reasons.

10 Accuracy of Data and Keeping Data Up-to-Date

10.1 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, as set out in Part 17, below.

10.2 The accuracy of personal data shall be checked when it is collected and at **every 4 to 6 weeks**. 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 that data, as appropriate.

11 Data Retention

11.1 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.

11.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

11.3 For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Policy.

12 Secure Processing

12.1 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.

12.2 All technical and organisational measures taken to protect personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data.

12.3 Data security must be maintained at all times by protecting the confidentiality, integrity, and availability of all personal data as follows:

12.3.1 only those with a genuine need to access and use personal data and who are authorised to do so may access and use it;

12.3.2 personal data must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed; and

12.3.3 authorised users must always be able to access the personal data as required for the authorised purpose or purposes.

13 Accountability and Record-Keeping

13.1 The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

13.2 The Company shall follow a privacy by design approach at all times when collecting, holding, and processing personal data. Data Protection Impact Assessments shall be conducted if any processing presents a significant risk to the rights and freedoms of data subjects (please refer to Part 14 for further information).

13.3 All employees, agents, contractors, or other parties working on behalf of the Company shall be given appropriate training in data protection and privacy, addressing the relevant aspects of Data Protection Law, this Policy, and all other applicable Company policies.

13.4 The Company's data protection compliance shall be regularly reviewed and evaluated by means of Data Protection Audits.

13.5 The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following:

13.5.1 the name and details of the Company, its Data Protection Officer, and any applicable third-party data transfers (including data processors and other data controllers with whom personal data is shared);

13.5.2 the purposes for which the Company collects, holds, and processes personal data;

- 13.5.3 the Company's legal basis or bases (including, but not limited to, consent, the mechanism(s) for obtaining such consent, and records of such consent) for collecting, holding, and processing personal data;
- 13.5.4 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;
- 13.5.5 details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
- 13.5.6 details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Policy);
- 13.5.7 details of personal data storage, including location(s); and
- 13.5.8 detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

14 Data Protection Impact Assessments and Privacy by Design

- 14.1 In accordance with privacy by design principles, the Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and where the processing involved is likely to result in a high risk to the rights and freedoms of data subjects.
- 14.2 The principles of privacy by design should be followed at all times when collecting, holding, and processing personal data. The following factors should be taken into consideration:
 - 14.2.1 the nature, scope, context, and purpose or purposes of the collection, holding, and processing;
 - 14.2.2 the state of the art of all relevant technical and organisational measures to be taken;
 - 14.2.3 the cost of implementing such measures; and
 - 14.2.4 the risks posed to data subjects and to the Company, including their likelihood and severity.
- 14.3 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:
 - 14.3.1 the type(s) of personal data that will be collected, held, and processed;
 - 14.3.2 the purpose(s) for which personal data is to be used;
 - 14.3.3 the Company's objectives;
 - 14.3.4 how personal data is to be used;
 - 14.3.5 the parties (internal and/or external) who are to be consulted;
 - 14.3.6 the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
 - 14.3.7 risks posed to data subjects;
 - 14.3.8 risks posed both within and to the Company; and
 - 14.3.9 proposed measures to minimise and handle identified risks.

15 Keeping Data Subjects Informed

- 15.1 The Company shall provide the information set out in Part 15.2 to every data subject:
- 15.1.1 where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
 - 15.1.2 where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
 - 15.1.3 if the personal data is used to communicate with the data subject, when the first communication is made; or
 - 15.1.4 if the personal data is to be transferred to another party, before that transfer is made; or
 - 15.1.5 as soon as reasonably possible and in any event not more than one month after the personal data is obtained.
- 15.2 The following information shall be provided in the form of a privacy notice:
- 15.2.1 details of the Company including, but not limited to, contact details, and the names and contact details of any applicable representatives and its Data Protection Officer;
 - 15.2.2 the purpose(s) for which the personal data is being collected and will be processed and the lawful basis justifying that collection and processing;
 - 15.2.3 where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;
 - 15.2.4 where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
 - 15.2.5 where the personal data is to be transferred to one or more third parties, details of those parties;
 - 15.2.6 where the personal data is to be transferred to a third party that is located outside of the EEA, details of that transfer, including but not limited to the safeguards in place (see Part 25 of this Policy for further details);
 - 15.2.7 details of applicable data retention periods;
 - 15.2.8 details of the data subject's rights under the Data Protection Legislation;
 - 15.2.9 details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;
 - 15.2.10 details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority');
 - 15.2.11 where the personal data is not obtained directly from the data subject, details about the source of that personal data;
 - 15.2.12 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; and
 - 15.2.13 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.

16 Data Subject Access

- 16.1 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.
- 16.2 Employees wishing to make a SAR should do so using a Subject Access Request Form, sending the form to the Company’s Data Protection Officer at admin@headstartaba.org 07535064745
- 16.3 Responses to SARs must normally be made within one month of receipt, however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.
- 16.4 All SARs received shall be handled by the Company’s Data Protection Officer.
- 16.5 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.

17 Rectification of Personal Data

- 17.1 Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.
- 17.2 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. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
- 17.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

18 Erasure of Personal Data

- 18.1 Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:
 - 18.1.1 it is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
 - 18.1.2 the data subject wishes to withdraw their consent to the Company holding and processing their personal data;
 - 18.1.3 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 21 of this Policy for further details concerning the right to object);
 - 18.1.4 the personal data has been processed unlawfully;
 - 18.1.5 the personal data needs to be erased in order for the Company to comply with a particular legal obligation; **OR**
 - 18.1.6 the personal data is being held and processed for the purpose of providing information society services to a child.
- 18.2 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. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

18.3 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).

19 Restriction of Personal Data Processing

19.1 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.

19.2 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).

20 Data Portability

20.1 The Company processes personal data using automated means within;

- Bright Hr
- Medesk
- Monday.com

20.2 Where data subjects have given their consent to the Company to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the Company and the data subject, data subjects have the right, under the Data Protection Legislation, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

20.3 To facilitate the right of data portability, the Company shall make available all applicable personal data to data subjects in the following format[s]:

- a) Email
- b) Printed paper.

20.4 Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

20.5 All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.]

21 Objections to Personal Data Processing

21.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests, for direct marketing (including profiling), [and processing for scientific and/or historical research and statistics purposes].

21.2 Where a data subject objects to the Company processing their personal data based on its 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.

21.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing promptly.

21.4 [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 the Data Protection Legislation, “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.]

22 Automated Processing, Automated Decision-Making, and Profiling

22.1 [The Company uses personal data in automated decision-making processes as follows:

- a) to discuss client progress
- b) company outcomes

22.2 [The Company uses personal data for profiling purposes as follows:

- a) To assess ethnicity of our clients
- b) To assess the ethnicity of our staff members

22.3 The activities outlined in this Part 22 are generally prohibited under the Data Protection Legislation where the resulting decisions have a legal or similarly significant effect on data subjects unless one of the following applies:

- a) the data subject has given their explicit consent;
- b) the processing is authorised by law; or
- c) the processing is necessary for the entry into, or performance of, a contract between the Company and the data subject.

22.4 If special category personal data is to be processed in this manner, such processing can only be carried out if one of the following applies:

22.4.1 The data subject has given their explicit consent; or

22.4.2 The processing is necessary for reasons of substantial public interest.

22.5 Where decisions are to be based solely on automated processing (including profiling), data subjects have the right to object, to challenge such decisions, request human intervention, to express their own point of view, and to obtain an explanation of the decision from the Company. Data subjects must be explicitly informed of this right at the first point of contact.

22.6 In addition to the above, clear information must be provided to data subjects explaining the logic involved in the decision-making or profiling, and the significance and envisaged consequences of the decision or decisions.

22.7 When personal data is used for any form of automated processing, automated decision-making, or profiling, the following shall apply:

- a) appropriate mathematical or statistical procedures shall be used;
- b) technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and
- c) all personal data to be processed in this manner shall be secured in order to prevent discriminatory effects arising.]

23 Direct Marketing

- 23.1 The Company is subject to certain rules and regulations when marketing its [products] **AND/OR** [services].
- 23.2 The prior consent of data subjects is required for electronic direct marketing including email, text messaging, and automated telephone calls subject to the following limited exception:
- a) The Company may send marketing text messages or emails to a customer provided that that customer's contact details have been obtained in the course of a sale, the marketing relates to similar products or services, and the customer in question has been given the opportunity to opt-out of marketing when their details were first collected and in every subsequent communication from the Company.
- 23.3 The right to object to direct marketing shall be explicitly offered to data subjects in a clear and intelligible manner and must be kept separate from other information in order to preserve its clarity.
- 23.4 If a data subject objects to direct marketing, their request must be complied with promptly. A limited amount of personal data may be retained in such circumstances to the extent required to ensure that the data subject's marketing preferences continue to be complied with.]

24 Personal Data Collected, Held, and Processed

Full details of the personal data collected, held, and processed by the Company are located in monday.com, Bright Hr, Medesk, data folder or paper form which is immediately destroyed. For details of data retention, please refer to the Company's Data Retention Policy.

25 Transferring Personal Data to a Country Outside the [UK and] EEA

- 25.1 The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the [UK and] EEA.
- 25.2 The transfer of personal data to a country outside of the [UK and] EEA shall take place only if one or more of the following applies:
- 25.2.1 the transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;
 - 25.2.2 the transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Data Protection Legislation); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
 - 25.2.3 the transfer is made with the informed and explicit consent of the relevant data subject(s);

- 25.2.4 the transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);
- 25.2.5 the transfer is necessary for important public interest reasons;
- 25.2.6 the transfer is necessary for the conduct of legal claims;
- 25.2.7 the transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
- 25.2.8 the transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

26 Data Breach Notification

- 26.1 All personal data breaches must be reported immediately to the Company's Data Protection Officer.
- 26.2 If an employee, agent, contractor, or other party working on behalf of the Company becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. Any and all evidence relating to the personal data breach in question should be carefully retained.
- 26.3 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.
- 26.4 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 26.3) 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.
- 26.5 Data breach notifications shall include the following information:
 - 26.5.1 The categories and approximate number of data subjects concerned;
 - 26.5.2 The categories and approximate number of personal data records concerned;
 - 26.5.3 The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);
 - 26.5.4 The likely consequences of the breach;
 - 26.5.5 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.

27 Implementation of Policy

This Policy shall be deemed effective as of <<insert date>>. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: Cynthia EwersCobb & Naomi Hantschar
Position: Operational Lead & Business and Finance Lead
Date: September 2020
Due for Review by: August 2021
Signature: