Action Homeless (Leicester) Ltd

Data Protection Policy

1. Policy statement and scope of policy

1.1 Action Homeless (Leicester) Ltd ("we", "our", "us", "the Company") have put together this policy to set out how we will use Personal Data.

1.2 This policy will apply to all employees, workers (including voluntary workers), consultants and trustees of the Company ("you" or "your"). It deals with how we handle the personal data of our customers, suppliers, employees, workers (including voluntary workers), consultants, trustees, job applicants, work experience students, fundraisers, contacts and other third parties.

1.3 When we make reference to an "individual" we refer to an individual whose personal data we are processing in accordance with this policy.

1.4 This policy does not form part of your contract of employment or engagement with the Company and may be amended at any time.

1.5 Any breach of this policy will be taken seriously and may result in disciplinary action. In some instances a serious breach of this policy may amount to gross misconduct and could result in the termination of your employment/engagement without notice or payment in lieu of notice or, if you are a trustee, the termination of your appointment.

1.6 It is intended that this policy will comply with the General Data Protection Regulation ("GDPR") and any UK supplemental legislation, including the Data Protection Act (2018) (together referred to as "the Data Protection Laws").

2. Understanding what Personal Data means

2.1 "**Personal Data**" means any information that identifies a living individual or relates to that individual. Examples include, but are not limited to information revealing their name, address, email address, identification number, location data, and online identifiers.

2.2 "**Special Categories of Personal Data**" are sensitive Personal Data which requires more careful processing in accordance with the Data Protection Laws. Special Categories of Personal Data means Personal Data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion or philosophical belief, and trade union membership. It also includes genetic and biometric data (where used for identification purposes).

2.3 "**Processing**" or **"Process**" for the purposes of this policy means any operation or set of operations which is performed on Personal Data. This includes collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, restriction, deletion or destruction. It includes transferring Personal Data to third parties.

3. Person responsible for data protection

3.1 The Company has appointed a person who is responsible for ensuring the Company's compliance with this policy and the Data Protection Laws. The current person responsible for data protection matters within the Company and their contact details are shown at the end of this document.

4. Personal Data protection principles

4.1 The Company adheres to the principles relating to Processing of Personal Data set out in the Data Protection Laws which require Personal Data to be:

4.1.1 Processed lawfully, fairly and in a transparent manner;

4.1.2 Collected only for specified, explicit and legitimate purposes;

4.1.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed;

4.1.4 Accurate and where necessary kept up to date;

4.1.5 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; and

4.1.6 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.

4.2 The Company is responsible for and will seek to demonstrate compliance with the above principles. This is referred to as "Accountability" in the Data Protection Laws.

5 Our lawful basis for the Processing of Personal Data

5.1 The Company will only collect, Process and share Personal Data fairly and lawfully and for specified purposes.

5.2 The Data Protection Laws set out the specified purposes ("Permitted Purposes") for which Personal Data may be Processed. The Company relies on one or more of the following Permitted Purposes when Processing Personal Data:

5.2.1 The Data Subject has given his/her consent;

5.2.2 The Processing is necessary for the performance of a contract with an individual (e.g. an employee);

5.2.3 The Processing is necessary to comply with the Company's legal obligations;

5.2.4 The Processing is necessary for the performance of a task carried out in the public interest;

5.2.5 The Processing is necessary in order to protect the vital interests of the individual; and/or

5.2.6 The Processing is necessary to pursue the Company's legitimate interests (or the legitimate interests of a third party (i.e. a benefits provider or pensions adviser)) where those legitimate interests are not overridden by the interests or fundamental rights and freedoms of the individual whose Personal Data we are Processing.

5.3 In addition to the Permitted Purposes set out in paragraph 5.2 above, the Data Protection Laws set out further additional specified purposes ("Additional Purposes") that the Company must be able to demonstrate if it wishes to Process Special categories of Personal Data. The Company will seek to rely on one or more of the following Additional Purposes when Processing Special categories of Personal Data:

5.3.1 The individual has given his/her explicit consent;

5.3.2 The Processing is necessary for carrying out the Company's rights and obligations under employment laws, social security laws or social protection laws;

5.3.3 The Processing is necessary to protect the vital interests of the individual or those of another person and where the individual is not physically or legally capable of giving Consent;

5.3.4 The individual has already made the Special categories of Personal Data public;

5.3.5 The Processing is necessary for the establishment, exercise or defence of legal claims;

5.3.6 The Processing is necessary for the purposes of occupational medicine or for the assessment of the working capacity of an employee, worker, or consultant;

5.3.7 The Processing is necessary for reasons of substantial public interest, on the basis of UK/EU law which shall be proportionate to the aim pursued, respect the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the individual; and/or

5.3.8 The Processing is necessary for archiving purposes in the public interest or for statistical purposes based on UK/EU law which shall be proportionate to the aim pursued, respect the essence of data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the individual. Those safeguards shall ensure that technical and organisational measures are in place in particular to ensure data minimisation and may include Pseudonymisation provided that those purposes can be fulfilled in that manner.

5.4 The Company will implement additional safeguards and security measures when Processing Special categories of Personal Data, and will ensure that access to such Data will be limited and restricted only to the Company's authorised HR personnel and, where necessary, employees responsible for the recruitment and management of employees, workers, and consultants and only then when it is necessary to make decisions, which include the consideration of such Personal Data as part of that decision-making process.

5.5 Information about criminal convictions

Because of the nature of the work we do (working with vulnerable adults and children) we are required to carry out criminal conviction checks of employees, workers, and volunteers (which may include trustees). This is in accordance with our obligations under the Safeguarding Vulnerable Groups Act 2006 (as amended by the Protection of Freedoms Act 2012) and under Part 1, Schedule 1 of the Rehabilitation of Offenders Act (Exceptions) Order 1975.

We may collect information about criminal convictions, if relevant and if legally required taking into the account the nature of the role and of the customers that we provide a service to. If this is relevant to you, we will inform you in advance and explain why this information is necessary.

We will ensure that we have in place appropriate safeguards when processing this type of information, and will seek to do so in accordance with our data protection policy.

We may use the Disclosure and Barring Service to make checks about criminal records relevant to the work we do and as required by law.

6 Consent for the Processing of Personal Data

6.1 The Company will only rarely and in exceptional circumstances request consent for the Processing of Personal Data/Special categories of Personal Data from its job applicants, employees, workers (including voluntary workers), consultants and trustees. In most cases, Processing will be carried out by the Company relying on one or more other Permitted Purposes or Additional Purposes.

6.2 In order for the Company to be able to rely on consent as a legal basis for Processing Personal Data it must be able to demonstrate that the consent is freely given, specific, informed and be an unambiguous indication of an individual's wishes which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

6.3 Any historical consent previously embedded in contracts of employment or otherwise which existed prior to the GDPR will no longer be relied on by the Company for the Processing of Personal Data or Special Categories of Personal Data.

6.4 Where consent is requested by the Company of its job applicants, employees, workers (including volunteers), trustees, or consultants for the purposes of Processing Personal Data, this will be on an entirely voluntary basis and will not be conditional on that individual's employment, work, consultancy, trustee position (as the case may be). Any request will also make it clear that consent can be withdrawn at any time and this will be easy to do. Any request for consent will make it clear what the consent is being sought for and will be kept separate from other terms and conditions of employment/engagement.

6.5 The Company will Process the Personal Data of its customers in accordance with any privacy notice issued to such customers (as referred to in paragraph 7 below). Where we require the consent of a customer we will do so in accordance with the GDPR.

6.6 The company will, where required, seek the consent of non-business contacts, consumer targets and other third parties to use their Personal Data for the purpose of marketing the Company's services and business.

6.7 If you need to request the consent of an individual to Process their Personal Data please speak to the person referred to in paragraph 3.1 to ensure that the correct procedure is used.

7 Privacy Notices

7.1 The Company is required to provide detailed, specific information to individuals when Personal Data is collected about them or whenever the reasons for Processing the Personal Data changes. The Company will provide this information to individuals in the form of privacy notices.

7.2 The Company's current privacy notice templates can be obtained from any Action Homeless managers or from its website. It is important that you use the correct one for the correct individual (e.g. Privacy Notice for Job applicants etc). It is important that these are issued to individuals at the point we collect any Personal Data regarding them. For the avoidance of doubt, privacy notices must be issued to our customers, suppliers, employees, workers, volunteers, consultants, job applicants, work experience students, and fundraisers if we are to receive any Personal Data from them. A failure to do so will mean that we are unlawfully processing Personal Data contrary to the Data Protection Laws.

8 Personal Data to be used only for specified purposes.

8.1 The Company will not use Personal Data for new, different or incompatible purposes from that disclosed in any privacy notice issued to an individual in accordance with paragraph 7 above.

8.2 In the event that the Company needs to Process Personal Data for new or different purposes from that disclosed, the Company will first issue a revised Privacy Notice to the affected individual explaining the change. Please contact the person referred to in paragraph 3.1 if this is required.

9 Use of Personal Data will be limited to what is necessary and will not be kept longer than needed

9.1 The Company will seek to ensure that the Personal Data Processed by the Company is adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed. It will not be stored for longer than it is needed.

9.2 Employees, workers (including volunteers), consultants and trustees may only Process Personal Data when performing their roles for the Company and the role requires such Processing. Processing of Personal Data is not permitted where such Processing is for any reason unrelated to their duties.

9.3 Employees, workers (including volunteers) consultants and trustees must only collect Personal Data that is necessary to fulfil their role for the Company. Excessive and irrelevant Personal Data must not be collected.

9.4 When Personal Data is no longer needed for specified purposes, the Company will delete such Personal Data or anonymise the Personal Data in accordance with the Company's Data retention guidelines and policies. Employees, workers, trustees and consultants are expected to follow such retention guidelines and policy when issued. If in doubt please contact the person referred to in paragraph 3.1.

9.5 The criteria used by the Company for determining how long Personal Data is retained for will generally be based on the following (without limitation):

9.5.1 The reason for holding the Personal Data in the first place;

9.5.2 How sensitive the Personal Data is;

9.5.3 Do we need the Personal Data for dealing with any litigation either for or against the Company;

9.5.4 Any laws that require us to keep Personal Data for specified periods;

9.5.5 Any limitation periods for claims against the Company;

9.5.6 Other reasons that may be relevant to our business.

10 We must ensure Personal Data is accurate and up-to-date

10.1 The Company will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant for the purpose for which we collected it. We will seek to check the accuracy of any Personal Data at the point of collection and at regular intervals thereafter. We will take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

10.2 Employees, workers (including volunteers), consultants and trustees who are required to Process Personal Data as part of their duties will abide by the principle set out in paragraph 10.1.

11 Security and confidentiality of Personal Data we Process

11.1 The Company has put in place appropriate IT security measures to protect Personal Data that is collected and used by the Company.

11.2 The Company also operates the following policies and procedures:

Internet and email usage policy

Data Protection Policy

11.3 The Company has put in place a variety of security and technical measures to protect the Company's systems and to protect against Personal Data security breaches, including but not limited to:

The Company collects and stores Personal Data in both paper and electronic format. All paper files are stored in locked cupboards and electronic data is held on secure servers. All Personal Data transmitted outside of the Company is password protected. The Company recognises that unauthorised or unlawful access, loss or destruction of Personal Data could cause damage or harm to the individual to who it relates and organises its data accordingly.

The person referred to in paragraph 3.1 is responsible for ensuring information security.

The Company's paper files are controlled and maintained by well trained employees and access to the files is restricted to the employees responsible for that file. The Company operates a clean desk policy and all paper files are locked in cupboards.

The Company's secure servers are located and backed-up within the EU and are secured with firewalls, antivirus software and security protocols. Access to the servers is by authorised employees only using secure passwords. Employees are well trained in the collection and use of the data, its access and sharing arrangements and will be trained on the contents of this Policy.

Employees been trained to respond to any breaches in data security by immediately reporting the breach to the person referred to in paragraph 3.1. The breach will, if appropriate be reported to the Information Commissioner and the individual(s) concerned. Any breach in data security will be treated as a serious incident. Employees, workers (including volunteers), consultants and trustees are responsible for protecting the Personal Data we hold and for ensuring that reasonable and appropriate security measures are used to prevent unlawful or unauthorised Processing of Personal Data or the accidental loss of, or damage to, Personal Data. Particular care must be exercised in protecting Special categories of Personal Data from loss and unauthorised access, use or disclosure.

11.4 Employees, workers (including volunteers), consultants and trustees must comply with all applicable aspects of the Company's IT security measures as referred to in paragraph 11.3 above and any other policies and procedures communicated from time to time regarding the Processing of Personal Data or IT security. Employees, workers (including volunteers), consultants and trustees will comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and other Data Protection Laws and relevant standards to protect Personal Data.

12 IMPORTANT: Reporting a Personal Data Breach

12.1 "Personal Data Breaches" are any acts or omissions that compromise the security, confidentiality, integrity or availability of the Personal Data or any safeguards either we, or any third party service providers have put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

12.2 The Company is required to notify the Information Commissioner of any Personal Data Breach within 72 hours of becoming aware of the Personal Data Breach save where the Personal Data Breach is unlikely to result in the risk to the rights and freedoms of natural persons.

12.3 All employees, workers, and consultants are expected to adhere to this paragraph 12. Any breach of this paragraph 12 will be taken seriously and may result in disciplinary action in relation to employees and other action in relation to non-employees. In some instances, serious breaches of

this paragraph 12 may be considered to be an act of gross misconduct which could result in the immediate termination of employment, or, as is the case, the immediate termination of any consultancy or engagement or appointment.

12.4 If you know or suspect that a Personal Data Breach has occurred you must immediately report this without delay to the person referred to in paragraph 3.1 (with a copy being sent to the Chief Executive Officer of the Company). To do so, you must either telephone or email him/her. The contact details appear below at the end of this Policy.

12.5 The information you should provide in paragraph 12.3 should where possible include a full description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of individuals concerned and the different types and approximate number of Personal Data concerned. You should also indicate whether you have taken any immediate measures in relation to the Personal Data Breach, and if so, what those measures are.

12.6 You must not report any Personal Data Breach direct to the Information Commissioner (unless involving your own Personal Data), and you must ensure that all reports required under this paragraph 12 are channelled through the person referred to in paragraph 3.1 and other authorised personnel in the first instance who will be responsible for investigating the matter and communicating with the Information Commissioner in this respect.

12.7 You must co-operate in full with any investigation carried out (whether carried out internally or externally and whether by the Company or Information Commissioner) into any Personal Data Breach and must comply promptly with all requests for information from the Company or the Information Commissioner in this respect.

12.8 Unless requested to do so by the Company, you must not attempt to investigate any known or suspected Personal Data Breach yourself. You should notify the person referred to in paragraph 3.1 (and other authorised personnel) immediately in accordance with paragraph 12.3 above and take instruction from that person and/or others authorised by him/her.

12.9 You must ensure that you preserve all evidence relating to any potential Personal Data Breach. You must not under any circumstances delete any such evidence without being authorised to do so, and in accordance with this policy and the Data Protection Laws.

12.10 You must report all forms of Personal Data Breach to the person referred to in paragraph 3.1 (and others if required) in accordance with this policy whether or not such Personal Data Breaches are of the type that need to be reported to the Information Commissioner. This includes any minor Personal Data Breaches.

12.11 The Company will maintain a record of all Personal Data Breaches, including minor Personal Data Breaches.

12.12 Employees, workers, consultants and trustees will, if appropriate be provided with training from time to time, in accordance with this policy. Such training shall include, but not be limited to how to recognise a Personal Data Breach, steps to take when reporting a Personal Data Breach and how to avoid Personal Data Breaches occurring. If you are unsure about what a Personal Data Breach might be or have any questions regarding Personal Data or how to report a Personal Data Breach you should contact the person referred to in paragraph 3.1.

13 Transfer of Personal Data outside the European Economic Area

13.1 The GDPR restricts data transfers to countries within the European Economic Area (EEA). The EEA is made up of all member states of the EU and Norway, Iceland and Liechtenstein.

13.2 In relation to Personal Data, the Company does not transfer any Personal Data outside the EEA and does not authorise any third party to do so.

14 Individual Rights

14.1 Individuals have rights when it comes to how we handle their Personal Data. These include rights to:

14.1.1 Withdraw consent to Processing at any time (if the Company is using consent as a legal basis for Processing the Personal Data);

14.1.2 Be informed about the Company's Processing activities. The Company complies with this right by issuing to individual's privacy notices from time to time (see paragraph 7 above);

14.1.3 Request access to their Personal Data held by the Company;

14.1.4 Prevent the Company's use of their Personal Data for direct marketing purposes;

14.1.5 Ask the Company to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate Data or to complete incomplete Data;

14.1.6 Restrict Processing in specific circumstances;

14.1.7 Challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

14.1.8 Request a copy of any agreement under which Personal Data is transferred outside the EEA;

14.1.9 Object to decisions based solely on automated Processing, including profiling;

14.1.10 Prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

14.1.11 Be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

14.1.12 Make a complaint to the Information Commissioner; and

14.1.13 In limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

14.2 Any request covered by paragraph 14.1 above should in the first instance be sent to the person referred to in paragraph 3.1.

15 Accountability

15.1 The Company has implemented appropriate technical and organisational measures in an effective manner, to ensure compliance with the Personal Data protection principles (for principles, see paragraph 4 above).

15.2 The Company, as Data Controller is responsible for, and will be able to demonstrate compliance with the Personal Data protection principles.

16 Record keeping

16.1 The Company will keep records of our Data Processing activities, including records of consents when required to in accordance with the Data Protection Laws.

17 Training

17.1 The Company will ensure that all employees, workers, consultants and trustees have undergone training to enable them to comply with the Data Protection Laws and this policy.

18 Automated Processing and Automated Decision-Making

18.1 Automated decision-making (decisions made based solely on automated Processing of Personal Data) will not be used by the Company when it has a legal or significant effect on an individual unless:

18.1.1 An individual has provided his or her explicit consent;

18.1.2 The Processing is authorised by law; or

18.1.3 The Processing is necessary for the performance of or entering into a contract.

18.2 If a decision is to be based solely on automated Processing (including profiling), then individuals will be informed.

19 Sharing Personal Data

19.1 Generally, the Company will only share Personal Data with third parties where certain safeguards and contractual arrangements have been put in place.

19.2 The Company will only share Personal Data held by the Company with third party service providers if:

19.2.1 They have a need to know the information for the purposes of providing the contracted services;

19.2.2 Sharing the Personal Data complies with any privacy notice issued in accordance with paragraph 7 above;

19.2.3 The third party has agreed to comply with our required data security standards, policies and procedures and has adequate security measures in place;

19.2.4 The transfer complies with any applicable cross border transfer restrictions; and

19.2.5 There is in place a written contract.

20 Changes to this policy

20.1 The Company reserves the right to change this policy at any time without notice.

Details of the current person responsible for data protection issues in the Company:

Reg Mawdsley
Finance Director
Action Homeless (Leicester) Ltd
Newton Lane
Wigston
Leics
LE18 3SE
Phone 0116 478 7531
Email: regmawdsley@actionhomeless.org.uk