Data Protection Policy
CANDARIN HOME LTD.

Last updated	

Definitions

Company	means Candarin Home Ltd, a UK registered company (no.08834290)
GDPR	means the General Data Protection Regulation.
Responsible Person	Means Ting Zhao.
Register of Systems	means a register of all systems or contexts in which personal data is processed by the Company.

1. Data protection principles
The Company is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. 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;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are 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 GDPR in order to safeguard the rights and freedoms of individuals; and
f. 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.

2. Consent

a. The Company must record service users' explicit consent to storing certain information (known as 'personal data' or 'special categories of personal data') on file.
b. For the purposes of the Regulations, personal and special categories of personal data include information relating to: (i) name and contact details; and (ii) genetic and/or biometric data which can be used to identify an individual.
c. Consent is not required to store information that is not classed as special category of personal data as long as only accurate data that is necessary for a service to be provided is recorded.
d. As a general rule, the Company will always seek consent where personal or special categories of personal information is to be held.
e. It should also be noted that where it is not reasonable to obtain consent at the time data is first recorded and the case remains open, retrospective consent should be sought at the earliest appropriate opportunity.

3. Obtaining Consent

a. Consent may be obtained in a number of ways depending on the nature of the interview, and consent must be recorded on or maintained with the case records:

- Face-to-face - A pro-forma should be used.
- Written - A pro-forma should be used.
- Telephone - Verbal consent should be sought and noted on the case record.
- Email - The initial response should seek consent.

b. Specific consent for use of any photographs and/or videos taken should be obtained in writing. Such media could be used for, but not limited to, publicity material, press releases, social media, and website. Consent should also indicate whether agreement has been given to their name being published in any associated publicity. If the subject is less than 18 years of age then parental/guardian consent should be sought.
c. Individuals have a right to withdraw consent at any time.

4. Ensuring the Security of Personal Information

a. It is an offence to disclose personal information 'knowingly and recklessly' to third parties.
b. It is a condition of receiving a service that all service users for whom we hold personal details sign a consent form allowing us to hold such information.

c. Service users may also consent for us to share personal or special categories of personal information with other helping agencies on a need to know basis.
d. A client's individual consent to share information should always be checked before disclosing personal information to another agency.
e. Where such consent does not exist information may only be disclosed if it is in connection with criminal proceedings or in order to prevent substantial risk to the individual concerned. In either case permission of the Managing Director should first be sought.

5. General provisions

a. This policy applies to all personal data processed by the Company.
b. The Responsible Person shall take responsibility for the Company's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.
d. The Company shall register with the Information Commissioner's Office as an organisation that processes personal data.

6. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the Company shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to the Company shall be dealt with in a timely manner.

7. Lawful purposes

a. All data processed by the Company must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).
b. The Company shall note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Company's systems.

8. Data minimisation

a. The Company shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

9. Accuracy

a. The Company shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

10. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the Company shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
b. The archiving policy shall consider what data should/must be retained, for how long, and why.

11. Security

a. The Company shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

12. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Company shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website). Please contact us first at: admin@unihood.com .

END OF POLICY