Data Protection Policy

Statement of Intent

Care4kids ltd are required to collect personal information for its employees, children, parents, other contacts, bill payers, other professionals and visitors. It is also necessary to process information so that children can be kept safe, be fully supported, and have their care and learning needs fully met; staff can be recruited and paid; activities organised; the business run efficiently and legal obligations to other bodies met. We intend to meet all the requirements of the Data Protection Act 1998 (the Act) and the General Data Protection Regulations 2018, and The Children Act 2006 (as defined by the EYFS Statutory Framework) when collecting, storing, and destroying personal data.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, **Care4kids ltd** must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 and the General Data Protection Regulations 2018. In summary these state that personal data must be:

- obtained and processed fairly and lawfully;
- obtained for a specified and lawful purpose and not processed in any manner incompatible with that purpose; adequate, relevant, and not excessive for that purpose;
- accurate and kept up to date;
- not kept for longer than is necessary;
- processed in accordance with the data subject's rights;
- kept safe from unauthorised access, accidental loss, or destruction;
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

As ever, we continue to take your privacy seriously, and in accordance with the General Data Protection Regulation.

We ask you for personal data about you, your child and the other emergency contacts. We must have a legal basis for collecting this data, and there are six lawful bases:

- **(a) Consent:** The individual has given clear consent for you to process their personal data for a specific purpose.
- **(b) Contract:** The processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- **(c) Legal obligation:** The processing is necessary for you to comply with the law (not including contractual obligations).
- **(d) Vital interests:** The processing is necessary to protect someone's life.
- **(e) Public task:** The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

- **(f) Legitimate interests:** The processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

We will be processing your data under the following bases:

Legal Obligation

For other matters, where we require consent, we will provide a way for you to positively make a decision about the information that you make available and how this is shared.

All of **Care 4 kids ltd** staff and volunteers who process or use any Personal Information must ensure that they follow these principles at all times. In order to ensure that this happens, Care 4 kids ltd has adopted this Data Protection Policy.

Notification of Data Held and Processed

All employees, volunteers, representatives, parents, visitors, and other members of the public have the right to:

- know what information Care 4 kids ltd holds and processes about them and why;
- know how to gain access to it;
- know how to keep it up to date;
- know what **Care 4 kids** are doing to comply with its obligations under the Act.

The Data Controller and the Designated Data Controllers

The **Care 4 kid's ltd** is the Data Controller under the Act, and the organisation is therefore ultimately responsible for implementation. However, Designated Data Controllers will deal with day to day matters. **Care 4 kids** Designated Data Controller is. **Michelle Newton.** In her absence, Kelly Farrell will act as Designated Data Controller.

Personal Information

Personal Information is defined as any details relating to a living, identifiable individual. Within **Care 4 kids ltd** this relates to employees; attending children and their families; other named contacts; bill payers; school representatives; volunteers; professional visitors; and some members of the public e.g. job applicants. We need to ensure that the information gained from each individual is kept securely and to the appropriate level of confidentiality.

The personal information collected from individuals could include:

- Their name
- Address
- Email address
- Telephone numbers-including those of emergency contacts
- Date of birth
- Medical information
- National Insurance number
- DBS numbers

- Bank account details
- Observations of children's progress (learning journals)
- Children's reports, from the setting or from outside professionals.
- Photographs (including videos)
- Family and individual medical history when necessary
- Continued Suitability
- Driving suitability
- Staff development records
- Learning and Development records of children
- Information shared about children by other professionals
- Accident / incident forms
- Emergency contact details designated by a person with parental responsibility.

Care 4 kids ltd store personal information to comply with the statutory framework (EYFS 2017); to deliver services to our families e.g. comply with our legal requirements as childcare providers; to employ suitable people for our setting; to run a sustainable business. The lawful reason for requiring this information always complies with article 6 of GDPR.

Processing of Personal Information

All staff and volunteers who process or use any Personal Information are responsible for ensuring that:

- Any Personal Information which they hold is kept securely
- Personal Information is not disclosed either orally or in writing or otherwise to any unauthorised third party
- Personal information is only used for the lawful purpose it was collected.

Staff and volunteers should note that unauthorised disclosure will be a disciplinary matter and may be considered gross misconduct in some cases.

Personal information will be:

- kept in a locked filing cabinet; or
- in a locked cupboard; or
- if it is computerised, be password protected;
- kept on a storage device which is itself kept securely.

Conversations and Meetings

Information of a personal or confidential nature should not be discussed in a public area, in front of anyone that is not an employee of the setting. Employees should be aware of confidentiality at all times when discussions are taking place, either distancing themselves from the conversation if it does not concern them, or, ensuring that their discussion is not overheard by others. All staff should respect the confidential nature of any information inadvertently overheard.

When meetings are being recorded it is important that only relevant information is written down. This must be carried out using the correct forms provided by the preschool, notes must be written legibly and coherently. The written notes are then to be stored in a locked cupboard and disposed of (shredded) in a timely manner as per the required time period for storage.

Collecting Information

Whenever information is collected about people, they should be informed why the information is being collected, who will be able to access it and to what purposes it will be put. The individual concerned must agree that he or she understands and gives permission for the declared processing to take place, or it must be necessary for the legitimate business of **Care 4 kids ltd**.

Sensitive Information

Sensitive information is defined by the Act as that relating to ethnicity, political opinions, religious beliefs, trade union membership, physical or mental health, sex life, criminal proceedings or convictions. The person about whom this data is being kept must give express consent to the processing of such data, except where the data processing is required by law for employment purposes or to protect the vital interests of the person or a third party.

Disposal of Confidential Material

Sensitive material should be shredded as soon as it is no longer needed; following retention guidelines and statutory requirements. Particular care should be taken to delete information from the tablets or the computer hard drive if they are to be disposed of.

Staff Responsibilities

All staff are responsible for checking that any information that they provide to Care 4 kids ltd in connection with their employment is accurate and up to date. Staff have the right to access any personal data that is being kept about them, either on computer or in manual filing systems. Staff should be aware of and follow this policy and seek further guidance where necessary.

Duty to Disclose Information

There is a legal duty to disclose certain information, namely, information about: child abuse/child protection, which will be disclosed to social services, or drug trafficking, money laundering or acts of terrorism or treason, which will be disclosed to the police.

Retention of Data

Care 4 kid's ltd takes care to only store personal information that is absolutely necessary. Personal information is kept for the period of time required for best practice, these retention periods are either recommended or statutory.

Stored information is filed in sealed filing boxes and securely stored or stored electronically and securely, including by **Care 4 kids ltd**. Once the retention period has lapsed, the information is destroyed.

For retention periods please see the Record Keeping & Retention Policy.

Third Party consideration

The information gathered may be shared with the following third-party companies:

- Inland Revenue
- I Connect / Parent Zone
- Boxed off Success (incl mail chimp)
- WhatsApp
- Facebook group (no images that could identify children)
- Ofsted
- Employment law consultants
- Slack
- Dropbox
- DBS service (including update service)
- For medical purposes
- CCTV
- School of child
- Other childcare providers where appropriate
- Direct Debit processing company
- World Pay
- Bank
- Any additional reputable company that the company decide to use.

When using third parties we will take all reasonable steps that they will be an effective data processor under GDPR and comply with all regulations.

The GDPR provides the following rights for individuals:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

Withdrawal of Consent

Individuals can withdraw consent for us to hold the data at any time, however, the requirements of the Children's Act 2006 and Safeguarding requirements will take precedence over GDPR.

All information is kept secure and any changes to information should be updated immediately on Parent Zone or by contacting the manager. The information will only be used for purposes described.

Every individual has the right to complain to the ICO (Information Commission Office)
Tel; 0303 123 1113.

Request for information held

Individuals can make a '**subject access request**' ('SAR') to find out the information we hold about them. This request must be made in writing. If we receive such a request we will forward it immediately to the Data Protection Officer/Data Protection Manager who will coordinate a response.

If you would like to make a SAR in relation to your own personal data you should make this in writing to the senior management team. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

In the unlikely event that there are and breaches of the GDPR requirements, ICO (Information Commission Office) will be notified as soon as practicable, and within 72 hours of that breach being discovered.