Data Protection Policy

What is Personal Data?

Personal data is described by the ICO as information that relates to an identified or identifiable individual.

What identifies an individual could be as simple as a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factors.

If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.

If you cannot directly identify an individual from that information, then you need to consider whether the individual is still identifiable. You should consider the information you are processing together with all the means reasonably likely to be used by either you or any other person to identify that individual.

Even if an individual is identified or identifiable, directly, or indirectly, from the data you are processing, it is not personal data unless it 'relates to' the individual.

When considering whether information 'relates to' an individual, you need to take into account a range of factors, including the content of the information, the purpose or purposes for which you are processing it and the likely impact or effect of that processing on the individual.

It is possible that the same information is personal data for one controller's purposes but is not personal data for the purposes of another controller.

Information which has had identifiers removed or replaced in order to pseudonymise the data is still personal data for the purposes of GDPR.

Information which is truly anonymous is not covered by the GDPR.

If information that seems to relate to a particular individual is inaccurate (ie it is factually incorrect or is about a different individual), the information is still personal data, as it relates to that individual.

GDPR sets out seven key principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Type of Data We Obtain

At the Nature Box, we collect:

- Emergency contact details of parents and details of any other emergency contact.
- Parent and Child Address
- Children's Allergy and medical information
- Children's Doctors information
- Parents Email Address.

How we Obtain and store Data

We obtain this information to ensure ultimate safety and care of the children. Parents contact information is paramount to ensure that they can be contacted at any point.

Children's Allergy and medical information is required to ensure our staff team can provide the best care.

Why We Obtain Data

We obtain data to ensure the safety of children within our care.

How Long We Keep Data For

Children and parent's personal data is stored until the child leaves our setting. Records of incidents, accidents, medication are stored for 10 years and are stored securely.

Sharing of Data with other agencies

Data Consent

Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation.

- We ask people to positively opt in.
- We do not use pre-ticked boxes or any other type of default consent.
- We use clear, plain language that is easy to understand.
- We specify why we want the data and what we are going to do with it.
- We give separate distinct ('granular') options to consent separately to different purposes and types of processing.
- We name our organisation and any third-party controllers who will be relying on the consent.
- We tell individuals they can withdraw their consent.
- We ensure that individuals can refuse to consent without detriment.
- We avoid making consent a precondition of a service.

Updating Personal Information

The Nature Box will ask for an update of information every 6 months. This is to ensure accuracy of information to continue to keep children safe throughout their time with us.

How Do we Keep Data Secure at The Nature Box?

All electronic information is stored on a password protected hard drive which is only accessed by management. Paperwork is stored in a lockable cabinet in a lockable room. Data stored for long periods of time, are filed into a lockable cabinet in a lockable room.

Staff Members and GDPR

All staff information is stored in a lockable cabinet in a lockable room. Staff are made aware of their GDPR rights in their contracts. We will ask staff to update their personal information every 6 months to ensure consistency and accuracy of information.

Staff Training and GDPR

All staff have access to online training around the topic of GDPR.

The Right to Withdraw Data

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.