Data Protection Policy

This policy represents the agreed principles for Data protection throughout the Nursery. All Nursery staff, representing Jack in the Box Nursery have agreed this policy.

At Jack in the Box, we aim to provide the highest quality education and care for all our children. We provide a warm welcome to each individual child and family and offer a caring environment where all children can learn and develop to become curious independent learners within their play.

Please read this policy in conjunction with all data protection policies for the information collected by Jack in the Box, the professionals this information may be shared with and the retention periods this data is held for.

Jack in the Box is fully committed to compliance with the requirements of the General Data Protection Regulation (GDPR) and all other data protection legislation currently in force. The Regulation applies to anyone processing personal data and sets out principles which should be followed and gives rights to those whose data is being processed. We keep several categories of personal data on our employees in order to carry out effective and efficient processes. We keep this data in a personal file relating to each employee and we also hold the data within our computer systems.

To this end, Jack in the Box endorses fully and adheres to the Data Protection Principles listed below. When processing data we will ensure that it is:

- processed lawfully, correctly, fairly and in a transparent way (‘lawfulness, fairness and transparency’)

- processed no further than the specific, explicit and legitimate purposes for which that data was collected (‘purpose limitation’) and limited to what is necessary for the purpose of processing.

- limited to what is necessary in relation to the purpose of processing (‘data minimisation’)

- accurate and kept up to date (‘accuracy’) Data which is found to be inaccurate will be rectified or erased without delay.

- kept in a form which permits identification of the data subject for no longer than is necessary (‘storage limitation’) for the purposes of processing.

- processed in a manner that ensures security of that personal data (‘integrity and confidentiality’) including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures.

- processed by a controller who can demonstrate compliance with the principles (‘accountability’)

These rights must be observed always when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, Jack in the Box will:

- observe fully the conditions regarding having a lawful basis to process personal information

- meet its legal obligations to specify the purposes for which information is used
- collect and process appropriate information only to the extent that it is necessary to fulfil operational needs or to comply with any legal requirements
- ensure the information held is accurate and up to date
- ensure that the information is held for no longer than is necessary
- ensure that the rights of people about whom information is held can be fully exercised under the GDPR (i.e. the right to be informed that processing is being undertaken, to access personal information on request; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as wrong information)
- take appropriate technical and organisational security measures to safeguard personal information
- ensure that personal information is not transferred outside the EU, to other countries or international organisations without an adequate level of protection and complies with GDPR procedures. Jack in the box does not transfer personal data to any recipients outside of the EEA.

EMPLOYEES PERSONAL INFORMATION

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors.

Throughout employment and for as long as is necessary after the termination of employment, Jack in the Box will need to process personal data about you. The kind of data that Jack in the Box will process includes:

- Staff name, address, date of birth, phone numbers
- DBS details
- any references obtained during recruitment, employment history, qualifications certificates, CV's, CV covering letters.
- details of terms of employment
- Bank details for payroll details for HMRC, such as name, address, income and pension information
- tax and national insurance information
- details of job duties (Job title/ Job description)
- details of health and sickness absence records
- details of holiday records/ attendance record
- information about performance/ Supervisions and Appraisals
- details of any disciplinary and grievance investigations and proceedings
- training records
- contact names and addresses/ copy of photographic ID
- correspondence with Jack in the Box and other information that you have given Jack in the Box

- emergency contact details
- It can also include pseudonymised data
- Nursery location

Jack in the Box believes that those records used are consistent with the employment relationship between Jack in the Box and yourself and with the data protection principles. The data Jack in the Box holds will be for management and administrative use only but Jack in the Box may, from time to time, need to disclose some data it holds about you to relevant third parties (e.g. where legally obliged to do so by HM Revenue & Customs, where requested to do so by yourself for the purpose of giving a reference or in relation to maintenance support and/or the hosting of data in relation to the provision of insurance)

DATA DISCLOSURE

Jack in the box may be required to disclose certain data/ information to any person. The circumstances leading to such disclosure include:

1. Any employee benefits operated by third parties.
2. Individuals with a disability- whether any reasonable adjustments are required to assist individuals in the setting or at work.
3. Individuals' health data- to comply with health and safety or occupational health obligations.
4. For statutory sick pay purposes.
5. HR management and administration- to consider how an individual's health affects their ability to do their job.
6. The smooth operation of any employee insurance, policies or pensions plans.
7. To assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect tax duty.

These kinds of disclosures will only be made when strictly necessary for the purpose.

Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain the company's commitment to protecting data.

In some cases, Jack in the Box may hold sensitive data, which is defined by the legislation as special categories of personal data, about you. For example, this could be information about health, racial or ethnic origin, criminal convictions, trade union membership, or religious beliefs. This information may be processed not only to meet Jack in the Box's legal responsibilities but, for example, for purposes of personnel management and administration, suitability for employment, and to comply with equal opportunity legislation. Since this information is considered sensitive, the processing of which may cause concern or distress, you will be asked to give express consent for this information to be processed, unless Jack in the Box has a specific legal requirement to process such data. We recognise the high standard attached to it's use. We understand that consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, we will do so on specific and individual basis where appropriate. Employees will be given clear instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

ACCESS TO DATA / EMPLOYEE RIGHTS

You have the following rights in relation to the personal data we hold on you:

1. The right to be informed about the data we hold on you and what we do with it
2. The right of access to the data we hold on you (see access to data below)
3. The right for any inaccuracies in the data we hold on you, however they came to light, to be corrected. This is also known as 'rectification'.
4. The right to have data deleted in certain circumstances. This is known as 'erasure'.
5. The right to restrict the processing of the data.
6. The right to transfer the data we hold on you to another party. This is known as 'portability'
7. The right to object to the inclusion of any information.
8. The right to regulate any automate decision making and profiling of personal data.

Employees have a right to access the personal data we hold on them. To exercise this right, employees should make a Subject Access Request (SAR). We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Employees, Parents/carers have to be proportionate and reasonable to allow the setting to run a focused search. If the focus is disproportionate, then we can ask for the scope of the search to be limited and advise will be taken from the Data Protection Officer (DPO). Consideration needs to be taken on the impact time/cost on an entire search and would it be reasonable to narrow the search down. Those who make a request will be kept fully informed of any decisions to extend the time limit.

No charge will be made for complying with a request unless the request is manifestly unfounded or excessive, or unless a request is made for duplicate copies to be provided. In these circumstances, a reasonable charge will be applied.

DATA SECURITY

You are responsible for ensuring that any personal data that you hold and/or process as part of your job role is stored securely.

You must ensure that personal information is not disclosed either orally or in writing, or via web pages, or by any other means, accidentally or otherwise, to any unauthorised third party.

You should note that unauthorised disclosure may result in action under the disciplinary procedure, which may include dismissal for gross misconduct. Personal information should be kept in a locked office, filing cabinet, drawer, or safe. Electronic data should be coded, encrypted, or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

When travelling with a device containing personal data, you must ensure both the device and data is password protected. The device should be kept secure and where possible it should be locked away out of sight i.e. in the boot of a car. You should avoid travelling with hard copies of personal data where there is secure electronic storage available. When it is essential to travel with hard copies of personal data this should be kept securely in a bag and where possible locked away out of sight i.e. in the boot of a car.

This policy was adopted by the managers and staff in September 2025

Signed on behalf of Jack in the Box Manager……

Staff Signatures: