Data Breach Policy for staff

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. Please read alongside Data Audit policy, General Data Protection Regulation policy and Data Retention 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.

As data controllers, Jack in the Box are responsible for keeping sensitive data about children, their families, and staff secure. If there is a data breach- loss of personal data- you must know what to do and how and when to report it to the Information Commissioners Office (ICO).

Some examples of data breaches:

A third-party accesses children or family data

For example- a visitor is found reading a child's or staff member's personal file.

This might mean- a child's medical status or staff member's details are misused.

Make it more secure- do not leave visitors unsupervised.

An accidental action leads to a data breach

For example- a staff member talks about a child to the wrong adult.

This might mean- a parent is given sensitive personal information about a child who is not their own.

Make it more secure- train staff to better manage busy handover periods.

Sending personal data to the incorrect recipient

For example- you send an email to the wrong person or send the wrong document to the wrong parent's house address.

This might mean- personal data about a child is shared with the wrong family

Make it more secure- always use BCC when sending group emails and double check before sending emails to individual recipients, double check contents of envelopes and send by recorded post.

Data breach on a computer, laptop, or tablet

For example- data is stolen through hacking or a laptop used to process children's data is lost or stolen.

This might mean- children's sensitive, personal data is stolen or misused.

Make it more secure- use a secure/ encrypted email provider and password protect documents which contain personal data.

Data is altered without permission

For example- a staff member accesses and updates a child's file without permission from the child's parents and/ or manager.

This might mean- you have failed to uphold the privacy principle of 'accuracy'

Make it more secure- train staff on GDPR and the implications if they make the wrong decision relating to children's data.

Loss of availability of data (short or long-term)

For example- an unencrypted memory stick or unlocked mobile phone is lost.

This might mean- children's sensitive, personal data is stolen and misused.

Make it more secure- encrypt and password protect all data storage software and hardware

Data is accessed by an inappropriate or unsuitable adult

For example- a staff member takes children's data home, and it is viewed by another adult who is disqualified to work with children.

This might mean- children's data is uploaded onto the dark web

Make it more secure- if staff are taking children's data home it needs to be locked away securely to ensure no one has access to the data

Identifying data that is shared online

For example, a child's photo is shared without parental permission, an email is sent to the wrong address; a child's name is shared on an online group, identifying information about a child or their family is put onto our Instagram page.

This might mean- confidentiality is broken because children's sensitive data is recognised by another person.

Make it more secure- think before you type! Do not include any identifying information about children, families, or staff on the internet.

What to do next….?

Record keeping

The data breach must be recorded- see attached Data Breach Record Form

ICO states that internal record keeping systems must be robust.

Reporting procedure

If there is a data breach- a loss of personal data- which will risk 'rights or freedoms' it must be reported within 72 hours (where feasible) to the ICO.

ICO reporting number -0303 123 1113

https://ico.org.uk/for-organisations/report-a-breach/

Parents must also be informed about the data breach if it is likely to risk their or their child's 'rights or freedom'

Risk assessment

Investigations might be carried out to review how the data breach occurred and to prevent future breaches. A Privacy Impact Assessment (risk assessment) should be completed.

Impact on the data controller

ICO have the power to fine the data controller.

Individuals- parents on behalf of their children or staff members- have the right to sue the data controller.

Taken form this article: - https://www.wordstream.com/blog/ws/2017/09/28/eu-gdpr.

'The first step of the process is a formal written warning, which can be issued to a company even in cases of unwitting violations; ignorance of the law is not a valid excuse for breaking it.

Firms that are found to have breaches or violated any part of the legislative package after initial sanctions can be fined up to 20 million euros (approximately $23.5 million USD) or 4% of a company's worldwide turnover, whichever is greater.

The next stage of punitive actions can force companies in violation of the GDPR to undergo regular periodic data integrity audits to ensure compliance, which also means surrendering access to potentially sensitive, confidential, or proprietary information to an auditor.'

This Policy was adapted by Jack in the box nurseries in September 2024

Signed on behalf of Jack in the box nurseries Manager

……

Staff signatures:

Data Breach Record Keeping

Date –

Data controller's name-

Type of data breach-
See examples of data breaches

Sensitivity of data-
How sensitive is the data breached?

Ease of identification of individuals-
How easy would it be for the data to allow identification of children or their families?

Severity of consequences for individuals-
How serious would it be if the data was misused?

Are vulnerable individuals affected? - Yes, data related to children and families.

How many individuals are affected? –
How many children and families are impacted by the breach?

Is the data sensitive? – Yes, data related to children and families.

Has the data breach been notified to –

ICO - YES / NO

Parent? - YES / NO

Privacy impact assessment
A risk assessment must be carried out to minimise the risk of a data breach occurring in the future.