Issued for:	Bordon Hill Nurseries	Number:	HR 004
Subject:	Data Protection Policy (inc GDPR)	Issue Date:	2020

Data Protection Policy & Procedure (including GDPR)

The Data Protection Policy is the responsibility of the Management Team who will control implementation of the policy.

Process Owner

Managing Director

Process Parties

Employees
Managers
Directors

Scope of Policy

The policy covers Bordon Hill Nurseries. It will be reviewed as and when required.

The purpose of this policy is to set out the Company's current procedure.

The Company reserves the right to alter any of the terms of this procedure at any time although changes will be notified to employees in writing following consultation.

Data Protection Policy

The GDPR (General Data Protection Regulation) came into force on 25 May 2018 and this regulation replaced the Data Protection Act 1998. Both employers and their employees have new responsibilities to ensure compliance.

Company's must have a valid reason for having personal data and the data should not be held for any longer than necessary. Below is further information on Data Processing and the GDPR.

What is GDPR?

The GDPR (General Data Protection Regulation) is concerned with respecting the rights of individuals when processing their personal information. This can be achieved by being open and honest with employees about the use of information about them and by following good data handling procedures.

The regulation contains 6 principles.

1. Personal data should be processed fairly, lawfully and in a transparent manner.
2. Data should be obtained for specified and lawful purposes and not further processed in a manner that is incompatible with those purposes.
3. The data should be adequate, relevant and not excessive.
4. The data should be accurate and where necessary kept up to date.
5. Data should not be kept for longer than necessary.

Data should be kept secure.All employees have a responsibility to ensure that their activities comply with the data protection principles. Line Managers have responsibility for the type of personal data they collect and how they use it. Staff should not disclose personal data outside the Company's procedures, or use personal data held on others for their own purposes.

Who does GDPR apply to?

The GDPR applies to any Company that handles personal data.

An individual who holds data about another individual on a personal level, for example a family members telephone number stored in a phone, will not need to consider GDPR for that particular data.

What is personal data?

Personal data is data that relates to an identified or identifiable individual and is:

a) processed electronically
b) kept in a filing system
c) part of an accessible record, for example an education record; or
d) held by a public authority.

This includes data that does not name an individual but could potentially identify them. For example, a payroll or staff number. Employees should be aware that any personal data you have in your possession will also be subject to the regulation. For example, if a Manager has a written copy of contact details for their team or an employee keeps customer names and numbers on post it notes on their desk.

A Company must have a lawful basis for handling any personal data.

How long can information be kept?

Information must not be kept for longer than is necessary.

While there is no set period of time set out within the GDPR, some records must be kept for a certain period of time in accordance with other legislation. For example, HMRC require payroll records to be kept for three years from the end of the tax year that they relate to.

To ensure its compliance to the GDPR, Bordon Hill Nurseries Limited must:

a) have a clear retention policy for handling personal data and ensure it is not held for longer than is necessary

b) have a legal basis for acquiring and/or using any personal data (further details of this can be found in our Privacy Statement)

c) ensure that all staff are aware of the retention policy and follow it

d) respond to subject access requests (sometimes called personal data requests) within one month

e) if there is a personal data breach that is likely to result in a risk to the rights and freedom of an individual, inform the Information Commissioners Office within 72 hours and, if the risk is deemed to be high, also inform the individual concerned.

Some employers will also be required to appoint a Data Protection Officer who can help embed, communicate and monitor the organisations GDPR data protection policies

An employee's right to request their personal data

Employees have a right to access information that the Company may hold on them. This could include information regarding any grievances or disciplinary action, or information obtained through monitoring processes.

If an employee wants to see their personal data, they should speak to their Manager in the first instance with a Subject Access Request. Most requests for personal data can be provided quickly and easily.

A Subject Access Request should be in writing and include:

a) full name, address and contact details

b) any information used by the Company to identify the employee (account numbers, unique ID's etc.)

c) details of the specific information required and any relevant dates.

The Company will respond to the Subject Access Request within one month of the request being made.

REVISION AND ISSUE STATUS

Data Protection Policy & Procedure (inc GDPR)

Issue No	Page No	Date Issued	Changes Made	Amended by
001	Whole Document		New Policy issued	