June 2018

Wishing Well Nursery

DATA PROTECTION POLICY

1. Introduction

This Data Protection Policy sets out how Wishing Well Nursery handles the Personal Data of our families, colleagues, and other third parties in compliance with the Data Protection Act 1998, and the General Data Protection Regulation 2018.

This Data Protection Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present.

2. Scope

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the nursery, and will provide our families and colleagues. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times.

The Owners of the Nursery are responsible for overseeing this Data Protection Policy and, as applicable, developing Related Policies and Data Protection Guidelines. That post is held by both Lynn Russell-Hubbard, and Linda Jessop, who can be contacted by telephone on 01922 767503.

Please contact the owners if you have any concerns that this Data Protection Policy is not being or has not been followed. In particular, you must always make contact in the following circumstances:

(a) if you are unsure of the lawful basis which you are relying on to process Personal Data

(b) if you are unsure about the retention period for the Personal Data being processed

(c) if you are unsure about what security or other measures you need to implement to protect Personal Data

(d) if there has been a Personal Data Breach

3. Personal data protection principles

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data Minimisation).

(d) Accurate and where necessary kept up to date (Accuracy).

(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is processed (Storage Limitation).

(f) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).

(g) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

4. Lawfulness and fairness

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject (for example children and families).

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing,

but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her Consent;

(Parental consent forms, parental agreement forms)

(b) the Processing is necessary for the performance of a contract with the Data Subject;

(Parental registration forms)

(c) to meet our legal compliance obligations;

(Early Years Statutory Framework, on the principles of Safeguarding)

(d) to protect the Data Subject's vital interests; or

(Health information, dietary requirements)

(e) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

(Recording of children's and parental views, opinions, and information to continually review our services)

You must identify and document the legal ground being relied on for each Processing activity.

5. Consent

A Data Controller (The Nursery Owners) must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

A Data Subject (Children and families) consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are not sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis, for example The Children's Act 2004, and therefore not require Explicit Consent to Process most types of Sensitive Data. Where Explicit Consent is required, you must issue a notice to the Data Subject to capture Explicit Consent. In all instances, this will be completed by the Nursery Owners.

6. Transparency (notifying data subjects)

The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, including registration forms and consent forms, we must provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller and D how and why we will use, Process, disclose, protect and retain that Personal Data, the best practice would be to signpost all parents, and colleagues to this policy.

When Personal Data is collected indirectly (for example, from a third party or publically available source), you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data (for example, private photographers). You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

7. Purpose limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be processed in any manner incompatible with those purposes.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have consented where necessary.

8. Data minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

You may only Process Personal Data where the performance of your job requires it. You cannot Process Personal Data for any reason unrelated to your job.

You may only collect Personal Data that you require for your job: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Society's data retention guidelines.

9. Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

10. Storage limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require. This includes requiring third parties to delete such data where applicable.

You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice or Fair Processing Notice.

11. Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

12. Reporting a Personal Data Breach

The GDPR requires Data Controllers to notify any Personal Data Breach to the Information Commissioner's Office (ICO) and, in certain instances, the Data Subject. If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for Personal Data Breaches and the DPM and follow the security incident response plan. You should preserve all evidence relating to the potential Personal Data Breach.

13. Data Subject's rights and requests

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) prevent our use of their Personal Data for direct marketing purposes;

(b) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

(c) restrict Processing in specific circumstances;

(d) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(e) request a copy of an agreement under which Personal Data is transferred outside of the EEA;

(f) object to decisions based solely on Automated Processing, including profiling

(g) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(h) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(i) make a complaint to the ICO; and

(j) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

14. Record keeping

The GDPR requires us to keep full and accurate records of all our data Processing activities.

You must keep and maintain accurate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

These records should include, at a minimum, the name and contact details of the Data Controller, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's

15. Sharing Personal Data

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with third parties, such as our children and families if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the Children's Act 2004, or other legal obligation.

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

16. Changes to this Data Protection Policy

We reserve the right to change this Data Protection Policy at any time without notice to you, so please check back regularly to obtain the latest copy of this Data Protection Policy.