

## **Data Protection Policy**

General Data Protection Regulation Policy Statement GDPR stands for General Data Protection Regulation and replaces the previous Data Protection Directives that were in place. It was approved by the EU Parliament in 2016 and came into effect on 25th May 2018. GDPR states that personal data should be 'processed fairly & lawfully' and 'collected for specified, explicit and legitimate purposes' and that individuals data is not processed without their knowledge and are only processed with their 'explicit' consent. GDPR covers personal data relating to individuals. Primrose Hill Day Nursery is committed to protecting the rights and freedoms of individuals with respect to the processing of children's, parents, visitors and staff personal data. The GDPR gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

### **GDPR includes 7 rights for individuals**

#### 1) The right to be informed

Primrose Hill Day Nursery is a registered Childcare provider with Northern Health and Social Care Trust and as so, is required to collect and manage certain data. We need to know parent's names, addresses, telephone numbers, email addresses, date of birth and National Insurance numbers. We need to know children's' full names, addresses, date of birth and Birth Certificate number. For parents claiming the free nursery entitlement we are requested to provide this data to Redbridge Council; this information is sent to the Local Authority via a secure electronic file transfer system. We are required to collect certain details of visitors to our nursery. We need to know visitor's names, telephone numbers, addresses and where appropriate company name. This is in respect of our Health and Safety and Safeguarding Policies. As an employer Primrose Hill Day Nursery is required to hold data on its employees; names, addresses, email addresses, telephone numbers, date of birth, National Insurance numbers, photographic ID such as passport and driver's license, bank details. This information is also required for company pension scheme as well as Disclosure and Barring Service checks (DBS) and proof of eligibility to work in the UK. This information is sent via a secure file transfer system to GPS Consultants for the processing of DBS checks.

#### 2) The right of access

At any point an individual can make a request relating to their data and Primrose Hill Day Nursery will need to provide a response (within 1 month). Primrose Hill Day Nursery can

refuse a request, if we have a lawful obligation to retain data i.e. from NHSCT in relation to the EYFS, but we will inform the individual of the reasons for the rejection. The individual will have the right to complain to the ICO if they are not happy with the decision.

### 3) The right to erasure

You have the right to request the deletion of your data where there is no compelling reason for its continued use. However, Primrose Hill Day Nursery has a legal duty to keep children's and parents details for a reasonable time, Primrose Hill Day Nursery retain these records for 6 years after leaving the nursery. Staff records must be kept for 6 years after the member of staff leaves employment, before they can be erased. This data is archived securely and shredded after the legal retention period.

### 4) The right to restrict processing

Parents, visitors and staff can object to Primrose Hill Day Nursery processing their data. This means that records can be stored but must not be used in any way, for example reports or for communications.

### 5) The right to data portability

Primrose Hill Day Nursery requires data to be transferred from one IT system to another; such as from Primrose Hill Day Nursery to the Local Authority/ Early Years Team. These recipients use secure file transfer systems and have their own policies and procedures in place in relation to GDPR.

### 6) The right to object

Parents, visitors and staff can object to their data being used for certain activities like marketing or research.

### 7) The right not to be subject to automated decision-making including profiling.

Automated decisions and profiling are used for marketing-based organisations. Primrose Hill Day Nursery does not use personal data for such purposes.

### **Storage and use of personal information.**

All paper copies of children's and staff records are kept in a locked filing cabinet in the office. Members of staff can have access to these files, but information taken from the files about individual children is confidential and apart from archiving, these records remain on site at all times. These records are shredded after the retention period. Information about individual children is used in certain documents, such as, a weekly register, medication forms, referrals to external agencies and disclosure forms. These documents include data such as children's names, date of birth and sometimes address. These records are shredded after the relevant retention period.

Primrose Hill Day Nursery collects a large amount of personal data every year including; names and addresses of those on the waiting list. These records are shredded if the child does not attend or added to the child's file and stored appropriately.

Information regarding families' involvement with other agencies is stored both electronically and in paper format, this information is kept in a locked filing cabinet in the office. These records are shredded after the relevant retention period. Upon a child leaving Primrose Hill Day Nursery and moving on to school or moving settings, data held on the child may be shared with the receiving school.

Primrose Hill Day Nursery stores personal data held visually in photographs or video clips, written consent is gained by parents/carers upon entry into the nursery. No names are stored with images in photo albums, displays, on the website or Primrose Hill Social media sites. Access to all the onsite computers are password protected. Any portable data storage used to store personal data, e.g. USB memory stick, are password protected and/or stored in a locked filing cabinet in the office.

**Data Protection Officer: Angela Magee**