**DATA PROTECTION POLICY-FORDFIELD NURSERY LTD**

The Nursery collects and uses certain types of personal information about staff, pupils, parents and individuals who come into contact with the Nursery in order to provide education and associated functions.

In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Education Authorities (LEASs), government agencies and other bodies, as a provider we are required to comply with the Data Protection Act 1998 and therefore are already collecting, maintaining, storing and possibly sharing the personal data of the children and families that we work with.

From 25th May 2018 Data Protection is changing and will be replaced by the EU General Data Protection Regulation (GDPR), making changes to how our nursery should process personal data.

According to the ICO personal data means data which relate to a living individual who can be identified –

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

**Principles of the GDPR**

The GDPR stipulates that anyone processing personal data must comply with six principles of good practice that are legally enforceable. The principles broadly require that personal information:

1. **Lawful** – the processing of personal data must be lawful and fair.
2. **Specified** purpose– the purpose for which personal data is collected on any occasion must be specified. Explicit and legitimate. Personal data must not be processed in a manner that is incompatible with the purpose for which it was collected.
3. **Appropriate** – personal data processed must be adequate, relevant and not excessive in relation to the purpose for which it was processed.
4. **Accurate** – personal data processed for any of the law enforcement process must be accurate and, where necessary, and that every reasonable step must be taken to ensure that personal data that is inaccurate is erased or rectified without delay.
5. **Time bound** – personal data processed must be kept for no longer than is necessary for the purpose for which it is being processed. Appropriate time limits must be established for the periodic review for the need for the continued storage of personal data for any of the law enforcement purposes.
6. **Secure** – personal data must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures.

**Personal data definitions**

The GDPR provides conditions for the processing of any personal data. It also makes a distinction between personal data and “sensitive” personal data.

Personal data is data from which a living individual can be identified from, for example name, ID number etc

Sensitive personal data is defined as personal data consisting of information about:

* Racial or ethnic origin
* Political opinion
* Religious or other beliefs
* Trade union membership
* Physical or mental health or condition
* Sexual life and
* Criminal proceedings or convictions

**Storage and security of personal data**

All appropriate steps will be undertaken to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

* Paper files and other records or documents containing personal data/sensitive data are kept in a secure environment
* Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically and individual passwords should be such that they are not easily compromised
* When personal data is required to be transferred to another personal, organisation, or third party all appropriate measures should be taken to maintain the appropriate security levels on that information
* Personal data should be readily available to a Data Subject upon request
* Personal data should be disposed of in accordance with the document retention schedule

**Communicating privacy information**

When we collect personal data we will communicate to individuals how we intend to use this information. Under GDPR these notices will include our legal basis for processing this data as well as how long we intend to retain it. We will also need to let you know that you can withdraw consent for your data to be held at any time, and that you have the right to complain to the ICO if you think there is a problem with the way we are handling your data.

**Individual rights**

The GDPR gives people who are having their personal data processed ‘Individual Rights’, on the whole they are the same as those under the DPA but with some enhancements.

The GDPR includes the following rights for individuals:

* The right to be informed
* The right of access
* The right to rectification
* The right to erasure
* The right to restrict processing
* The right to data portability
* The right to object; and
* The right not to be subject automated decision-making including profiling. You can find them on the ICO website: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/>

**Lawful basis for processing personal data**

One of the key points of GDPR is that we must have a lawful basis for processing personal data. A lawful basis means ‘a reason’. The reason needs to be legally defensible (so not just ‘because you thought it was a good idea’). There are 6 potential lawful basis:

**Consent**

Parents must give their consent for the setting to process personal data for a specific purpose.

**Contract**

Parents will be asked to agree a contract with the setting and the necessary data will be processed by us. Parents may ask us to take specific steps before entering into a contract.

**Legal obligation**

When processing data, we must comply with the law (this does not include contractual obligations).

**Vital interests**

The processing is necessary to protect someone’s life.

**Public task**

Processing is necessary to perform a task in the public interest or for our official functions, e.g. open days, and the task or function has a clear basis in law.

**Legitimate interests**

Processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests.

**Subject access requests**

This is when an individual requests a copy of the information held about them; Under GDPR if we receive such a request, we will need to respond within a month.