



The Children's House Montessori Nursery

Data Protection Policy

At The Children's House we adhere to the General Data protection Regulations (GDPR) 2018. These regulations state we are required to collect process and retain certain types of information and personal data in order to comply with legislation relating to our business. This includes any Data stored either in paper form or on an electronic device.

This policy relates to the protection of this data and how this personal data must be handled to protect the privacy of those it concerns.

The nursery needs to collect certain types of information about employees, children, parents and any other individuals who come into contact with the nursery in order to operate efficiently. Only relevant personal data may be collected and the person collecting the data should be informed of the data's intended use.

The Children's House regards the lawful and correct treatment of personal data to be of paramount importance. All individuals associated with our setting have the right to expect that their personal data is treated lawfully and respectfully. To ensure this we adhere to the principles of the General Data Protection Regulations (GDPR) 2018 and other guidelines for the collection and processing of personal data.

The GDPR principles require that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Collected for specified explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In addition Article 5 (2) requires that:

- The controller shall be responsible for, and be able to demonstrate, compliance with the principles
(Source: The Information Commissioner's Office)

We as a setting have responsibilities to protect any data we retain for our records. To ensure these responsibilities are upheld a Data Protection Lead (DPL) has been appointed to monitor all aspects of data protection. This person is Laura Elrick. Additionally, we have registered with the information commissioner's office (ICO). Our DPL regularly checks all data is correct and our systems are protected. It is their responsibility to complete annual audits on our processes and to monitor staff with regards to appropriate data handling.

Along with this policy we have privacy notices for both employees and parents detailing how we comply with GDPR and fulfil our obligations in ensuring we are compliant with legislation relating to our business.

All personal data obtained must be stored in a secure and safe manner and only management may access personnel files. All electronic data must be password protected and firewall systems should be in place on any device containing sensitive information including systems such as Tapestry. (Please see our Tapestry policy for more information).

Parents will be regularly reminded to update any personal information relating to their child including telephone numbers, change of address or home situation. Any personal information including Learning Journals must have parental permission before being shared with any other person's or agency. This includes any transfer of information from one setting to another. Any requests made by telephone to receive data must be checked with the manager to ensure that person is entitled to receive the data requested. No personal data will be used on social media, nursery websites or in newsletters without prior consent from the data subject. This consent must be in writing before any data is shared. Parents are informed of their right to withdraw their consent and the right to the information we hold. Parents are informed that they have the right to access any personal data and that any inaccurate data be updated or deleted. All such requests must be made in writing to the Data Protection Lead (DPL).

Staff receive training for our processes on data handling and are appropriately supervised when accessing any data related to employees, parents or children.

Staff are made aware that any breach of data protection will result in disciplinary action being taken against them.

Data sharing agreements are in place for those agencies requiring us to share information with them regarding any children or employees at the setting. Additionally they are given a copy of our data protection policy.

Our email systems are password protected and these are only known by the management team. Any breach of our passwords by a member of staff will result in our passwords being changed immediately. (Please see our internet policy for more information)

All devices where information is stored are password protected to prevent any unauthorised access.

Any information we hold may be shared without prior consent if there is evidence that a child is suffering, or at risk of significant harm, there is reason to suspect that a child may be suffering or to prevent a crime from being committed, or when not sharing the information could be worse than the outcome of sharing it

If parents or employees wish to make a complaint about how their data is being held they should go direct to the DPL in the first instance. If they are still dissatisfied after raising a concern they can make a complaint to the information Commissioners Office (ICO) by writing to Information Commissioners Officer, Wycliffe House, Water lane, Wilmslow, Cheshire SK9 5AF or via their website ico.org.uk