**GDPR and Data Protection Policy**

General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) is the law that protects personal privacy and upholds individual’s rights.  It applies to anyone who handles or has access to people’s personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

**Privacy Notice**

At Moniques Montessori day nursery we take privacy very seriously and we meet the data protection standards encapsulated in the GDPR (General Data protection regulation).

We are registered with the information commissioner’s office (ICO).

The categories of information that we collect, hold and share include:

* Personal information  (name, address, date of birth)
* Characteristics (ethnicity, language, nationality, country of birth, eligibility for early years pupil premium)
* Attendance information
* Observations and assessment information
* Developmental progress tracking
* Medical information
* Special educational needs and disabilities information
* Referrals and liaison with other relevant services
* Safeguarding information

We also collect, hold and share some information on children’s parents, guardians and significant others including :

* Personal information
* National Insurance numbers

We use the children’s and parents’ data to:

* Support the child’s learning and development
* Enabling planning of suitable activities to extend knowledge and skills
* Ensure children’s safety within the childcare provision
* Monitor and report on children’s progress
* Provide behavioural and emotional support when required
* Evaluate the quality of our service as a childcare provider
* Comply with the law regarding data collection and sharing
* Meet the requirements of the early years foundation stage
* Make claims for funding

We collect and use children’s information under the following lawful bases :

* to meet our contractual obligations regarding the provision of childcare and, where applicable, to provide funded childcare to eligible families
* to meet our legal obligation to comply with the law, for example, the early years census

While the majority of children’s information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the GDPR, we will inform you when you are required to provide certain children’s information to us, or if you have a choice.

We are required to hold children data for a reasonable period of time after children have left the provision as a requirement under the EYFS, for example, until after the next OFSTED inspection.  The limitation act 1980 recommends that we retain data until the child reaches the age of 21 or, until the child reaches the age of 24, for child protection records.

Your data will be held securely and will only be accessible by staff who are authorised to do so. We routinely share our children’s information with:

Schools that the child attends after leaving out provision

Other childcare providers the child is engaged with currently

The local authority for funding claims and the early years census

The department of education annual early years census

Special educational needs coordinator as appropriate or required

NHS Services, health visitors, speech and language therapists

We do not share information about our children with anyone without your consent or knowledge, **unless** the law or our policies allow us to do so. However, we do share our children’s data with the department of education on a statutory basis, and we are required to submit data to Kent local authority, for them to aggregate and submit as part of the annual early years census in January and, where applicable, to access child care funding.

To be granted access to children’s information, organisations (such as the local authority) must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

Under data protection legislation, parents and children have the right to request access to information about them that we hold.  To make a request for your personal information, or be given access to your child’s early years record, contact Stefanie Purdy, nursery business manager.

In law, you have the right to:

* Object to processing of personal data that is likely to cause, or is causing damage or distress
* Prevent processing for the purpose of direct marketing
* Have inaccurate personal data rectified, blocked, erased or destroyed
* Claim compensation for damage is caused by any breach of the data protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance.  Alternatively, you can contact the information commissioner’s office directly.

**Policy Objectives**

The nursery as the Data Controller will comply with its obligations under the GDPR and DPA.  The nursery is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation.

All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted.  All staff must read, understand and comply with this policy.

The Information Commissioner as the Regulator can impose fines of up to 20 million Euros (approximately £17 million) for serious breaches of the GDPR, therefore it is imperative that the  and all staff comply with the legislation.

**Scope of the Policy**

Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information.  The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual.  This includes any expression of opinion about an individual and intentions towards an individual.  Under the GDPR personal information also includes an identifier such as a name, an identification number, location data or an online identifier.

The Nursery collects a large amount of personal data every year including: pupil records, staff records, names and addresses of those requesting prospectuses, references, fee collection data used by the Nursery.  In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

**The Principles**

The principles set out in the GDPR must be adhered to when processing personal data:

1. Personal data must be processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**)
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**)
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (**data minimisation**)
4. Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (**accuracy**).
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed (**storage limitation**)
6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information are processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (**integrity and confidentiality**).

**Transfer Limitation**

In addition, personal data shall not be transferred to a country outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data as determined by the European Commission or where the organisation receiving the data has provided adequate safeguards.

This means that individuals’ rights must be enforceable and effective legal remedies for individuals must be available following the transfer.  It may also be possible to transfer data where the data subject has provided explicit consent or for other limited reasons.  Staff should contact the DPO (Stefan Purdy) if they require further assistance with a proposed transfer of personal data outside of the EEA.

**Sensitive Personal Information**

Processing of sensitive personal information (known as ‘special categories of personal data’) is prohibited unless a lawful special condition for processing is identified.

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:

* There is a lawful basis for doing so as identified on previous page
* One of the special conditions for processing sensitive personal information applies:
1. the individual (‘data subject’) has given explicit consent (which has been clearly explained in a Privacy Notice)
2. the processing is necessary for the purposes of exercising the employment law rights or obligations of the school or the data subject
3. the processing is necessary to protect the data subject’s vital interests, and the data subject is physically incapable of giving consent
4. the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim
5. the processing relates to personal data which are manifestly made public by the data subject
6. the processing is necessary for the establishment, exercise or defence of legal claims
7. the processing is necessary for reasons of substantial public interest
8. the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services
9. the processing is necessary for reasons of public interest in the area of public health.

The nursery’s privacy notice(s) set out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Unless the nursery can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data.  Evidence of consent will need to be captured and recorded so that the nursery can demonstrate compliance with the GDPR.

**Privacy Notice**

The nursery will issue privacy notices as required, informing data subjects (or their parents, depending on age of the pupil, if about pupil information) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the GDPR including the identity of the DPO, how and why the nursery will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data).

When information is collected indirectly (for example from a third party or publicly available source) the data subject must be provided with all the information required by the GDPR as soon as possible after collecting or receiving the data.  The nursery must also check that the data was collected by the third party in accordance with the GDPR and on a basis which is consistent with the proposed processing of the personal data.

The nursery will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The nursery will issue a minimum of two privacy notices, one for pupil information, and one for workforce information, and these will be reviewed in line with any statutory or contractual changes.  Follow this link to the GDPR page on KELSI where you will find the model privacy notice(s) for nurserys to use: <http://www.kelsi.org.uk/school-management/data-and-reporting/access-to-information/the-general-data-protection-regulation-gdpr>

**Data minimisation**

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

Staff may only process data when their role requires it.  Staff must not process personal data for any reason unrelated to their role.

The nursery maintains a Retention Schedule (APPENDIX 4) to ensure personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time.  Staff must take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required in accordance with the Schedule.  This includes requiring third parties to delete such data where applicable.

Staff must ensure that data subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

**Individual Rights**

Staff as well as any other ‘data subjects’ have the following rights in relation to their personal information:

* To be informed about how, why and on what basis that information is processed *(see the relevant privacy notice)*
* To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request *(see Appendix 1 - Procedure for Access to Personal Information)*
* To have data corrected if it is inaccurate or incomplete
* To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (‘the right to be forgotten’)
* To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where the nursery no longer need the personal information, but you require the data to establish, exercise or defend a legal claim
* To restrict the processing of personal information temporarily where you do not think it is accurate (and the nursery are verifying whether it is accurate), or where you have objected to the processing (and the nursery are considering whether the nursery’s legitimate grounds override your interests)
* In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format
* To withdraw consent to processing at any time (if applicable)
* To request a copy of an agreement under which personal data is transferred outside of the EEA.

* To object to decisions based solely on automated processing, including profiling
* To be notified of a data breach which is likely to result in high risk to their rights and obligations
* To make a complaint to the ICO or a Court.

**Individual Responsibilities**

During their employment, staff may have access to the personal information of other members of staff, suppliers, clients or the public.  The nursery expects staff to help meet its data protection obligations to those individuals.

If you have access to personal information, you must:

* only access the personal information that you have authority to access and only for authorised purposes
* only allow other staff to access personal information if they have appropriate authorisation
* only allow individuals who are not nursery staff to access personal information if you have specific authority to do so
* keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the nursery’s policies).
* not remove personal information, or devices containing personal information (or which can be used to access it) from the nursery’s premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device
* not store personal information on local drives or on personal devices that are used for work purposes.

**Information Security**

The nursery will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All staff are responsible for keeping information secure in accordance with the legislation and must follow the nursery’s acceptable usage policy.

The nursery will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the **confidentiality, integrity and availability** of the personal data, defined as follows:

**Confidentiality** means that only people who have a need to know and are authorised to use the personal data can access it.

**Integrity** means that personal data is accurate and suitable for the purpose for which it is processed.

**Availability** means that authorised users can access the personal data when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the nursery has implemented and maintained in accordance with the GDPR and DPA.

Where the nursery uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information.  Contracts with external organisations must provide that:

* the organisation may only act on the written instructions of the nursery
* those processing data are subject to the duty of confidence
* appropriate measures are taken to ensure the security of processing
* sub-contractors are only engaged with the prior consent of the nursery and under a written contract
* the organisation will assist the nursery in providing subject access and allowing individuals to exercise their rights in relation to data protection
* the organisation will delete or return all personal information to the nursery as requested at the end of the contract
* the organisation will submit to audits and inspections, provide the nursery with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the nursery immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

**Storage and retention of personal information**

Personal data will be kept securely in accordance with the nursery’s data protection obligations.

Personal data should not be retained for any longer than necessary.  The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained.  Staff should adhere to the KCC Information Management Toolkit for Nurseries on KELSI with reference to the Record Retention Schedule, available at the following link:  [http://www.kelsi.org.uk/\_\_data/assets/word\_doc/0012/60213/InformationManagementToolkitforNurserysv4-2.docx](http://www.kelsi.org.uk/__data/assets/word_doc/0012/60213/InformationManagementToolkitforSchoolsv4-2.docx)

Personal information that is no longer required will be deleted in accordance with the Nurseries Record Retention Schedule (APPENDIX 4).

**Data breaches**

A data breach may take many different forms:

* Loss or theft of data or equipment on which personal information is stored
* Unauthorised access to or use of personal information either by a member of staff or third party
* Loss of data resulting from an equipment or systems (including hardware or software) failure
* Human error, such as accidental deletion or alteration of data
* Unforeseen circumstances, such as a fire or flood
* Deliberate attacks on IT systems, such as hacking, viruses or phishing scams
* Blagging offences where information is obtained by deceiving the organisation which holds it

The nursery must report a data breach to the Information Commissioner’s Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals.  The nursery must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Staff should ensure they inform their line manager/DPO/Registered person immediately that a data breach is discovered and make all reasonable efforts to recover the information, following the nursery’s agreed breach reporting process.

**Training**

The nursery will ensure that staff are adequately trained regarding their data protection responsibilities.

**Consequences of a failure to comply**

The nursery takes compliance with this policy very seriously.  Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the nursery and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under the nursery’s procedures and this action may result in dismissal for gross misconduct.  If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact your line manager or the nursery’s DPO.

**Review of Policy**

This policy will be updated as necessary to reflect best practice or amendments made to the GDPR or DPA.

In meeting the needs of all the children in our care it is important to share information with parents and with one another in order to support the child’s development.    It may also be necessary in some circumstances for the nursery to seek help and advice from outside professionals.   If this action is taken the parent’s permission will first be sought, except where this is precluded through child protection considerations.

Any information and knowledge will be on a need to know basis and will be kept confidential.

No unnecessary information will be collected and retained beyond its useful (or legal requirement) period.

We keep two kinds of records on the children attending our setting:

* Developmental records - Montessori records, reports, observations and drawings etc.
* Personal records - registration forms, consent forms, emergency contacts, significant others and correspondence concerning the child.

We also keep records on staff, equipment, environmental health etc. (see policy on Essential records).

Parents may request access to any records held on their child and family with the exception of the Safeguarding and Child Protection Folder. In the interest of the child, the manager reserves the right to be selective as to who should see what. The setting commits to providing access within 1 week. If the setting declines an application, reasons will be provided.