65. General Data Protection Policy

Statement of Intent

The General Data Protection Regulation (GDPR) is designed to protect the privacy of individuals. It requires that any personal information about an individual is processed securely and confidentially. This includes both staff and children. How Montessori & Me obtains, shares and uses information is critical, as personal data is sensitive and private. Everyone, adults and children alike, have the right to know how the information about them is used. The General Data Protection Regulation requires the setting to strike the right balance in processing personal information so that an individual's privacy is protected. Applying the principles to all information held by the Montessori & Me will typically achieve this balance and help to comply with the legislation.

We will respect the privacy of children and their parents/carers, while ensuring that they access high quality early years care and education in our setting. We aim to ensure that all parents/carers can share their information in the confidence that it will only be used to enhance the welfare of their children. There are record keeping systems in place that meet legal requirements; means of storing and sharing that information take place within the framework of the General Data Protection Regulation and the Human Rights Act.

General Data Protection Regulation principles

To comply with the act, the setting must observe the 'General Data Protection Regulation principles', ensuring that:

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area 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.

In practice, it means that Montessori & Me must:

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how they intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways they would reasonably expect; and
- make sure they do not do anything unlawful with the data

Personal data is information that relates to an identifiable living individual that is processed as data. Processing amounts to collecting, using, disclosing, retaining or disposing of

information. The General Data Protection Regulation principles apply to all information held electronically or in structured paper files.
The principles also extend to educational records – the names of staff and children, dates of birth, addresses, national insurance numbers, development outcomes within the EYFS, medical information, SEN assessments and staff development reviews.
Sensitive personal data is information that relates to

- race and ethnicity,
- political opinions,
- religious beliefs,
- physical and mental health,
- sexuality
- criminal offences

Sensitive personal data is given greater legal protection as individuals would expect certain information to be treated as private or confidential – for example, a nursery manager may have a pre-school e-mail account that is made publicly available on the nursery's website whereas their home e-mail account is private and confidential and should only be available to those to whom consent had been granted. It is important to differentiate between personal information that individuals would expect to be treated as private or confidential (whether or not legally classified as sensitive personal data) and personal information you can make freely available. For example: the manager's identity is personal information, but everyone would expect it to be publicly available. However, the manager's home phone number would usually be regarded as private information.

What must the setting do?

- We must notify the ICO (Information Commissioner's Office) that we are processing personal data.
- We have a nominated individual as the 'Data Protection Controller'.
- The setting has clear, practical policies and procedures on information governance for staff to follow and needs to monitor their operation.
  These should include:
  - Staff Code of Conduct
  - Privacy notices for staff and parents/children
  - Record Management Policy (not mandatory, but good practice)
  -

Data Breaches – In the event of a personal data breach, the Data Protection Controller should be notified immediately and an investigation carried out.

Individual Rights

The General Data Protection Regulation 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 to automated decision-making including profiling.

The General Data Protection Regulation entitles an individual the right to request the personal information a setting holds on their behalf – this is known as a Subject Access Request (SAR)

and includes all and any information held by the setting, not just that information held on central files or electronically, so it could also include correspondence or notes held by others in the setting. If you would like a copy of your personal information, you should contact the setting Manager. You may need to pay to cover our administration costs.

- SARs must be responded to within 1 month of receipt.
- The SAR should be made in writing by the individual making the request.
- The setting can refuse or charge for requests that are manifestly unfounded or excessive
- Parents can make SARs on behalf of their children if the children are deemed to be too young or they have consented to their parents doing so on their behalf.

Storage and use of personal information

All paper copies of children's and staff records are kept in a locked filing cabinet in Montessori & Me. 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.
Montessori & Me 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 on icloud and in paper format, this information is kept in a locked filing cabinet in the setting. These records are shredded after the relevant retention period.
Upon a child leaving Montessori & Me and moving on to school or moving settings, data held on the child may be shared with the receiving school. Such information will be sent via hard copies given directly to the receiving school or through secure Royal Mail, special delivery.
Montessori & Me stores personal data held visually in photographs or video clips or as sound recordings, unless no written consent has been obtained via Registration form. No names are stored with images in photo albums, on the website or on the settings social media site.
Access to all setting computers and Tapestry Online Learning Journal is password protected. When a member of staff leaves Montessori & Me these passwords are changed in line with this policy and our Safeguarding policy. 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.

GDPR means that Montessori & Me;

- Manage and process personal data properly
- Protect the individual's rights to privacy
- Provide an individual with access to all personal information held on them

Please see attached Preschool Learning Alliance Retention periods for records.

Staff Responsibilities

Staff need to know and understand:

- How to manage, keep and dispose of data
- The settings procedures in relation to children's records, email, social media, taking photos in the setting, mobile technology and the settings website
- When they are allowed to share information with others and how to make sure it is kept secure when shared.

Information and IT Equipment Acceptable Usage

Acceptable Usage covers the security and use of all Montessori & Me pre-school IT equipment. This applies to all information, in whatever form, relating to the settings activities, and to all information handled by Montessori & Me relating to other organisations with whom it deals.

Computer Access Control – Individual's Responsibility

Access to the Montessori & Me IT systems is controlled by the use of User IDs and passwords. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the settings IT systems.

Individuals must not:

- Allow anyone else to use their user ID and password on any Montessori & Me IT system.
- Leave their user accounts logged in at an unattended and unlocked computer whilst in the setting.
- Access Montessori & Me IT systems outside of the setting.
- Use someone else's user ID and password to access the settings systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to Montessori & Me IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Store Montessori & Me data on any non-authorised IT equipment.
- Give or transfer the settings data or software to any person or organisation outside Montessori & Me without the authority of the setting manager.

The setting manager and deputy must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

Internet and email Conditions of Use

Use of Montessori & Me internet and email is intended for business use only. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to the setting in any way, not in breach of any term and condition of employment and does not place the individual or Montessori & Me in breach of statutory or other legal obligations. All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications
- Access, download, send or receive any data (including images), which Montessori & Me considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal business
- Use the internet or email to gamble
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to Montessori & Me, alter any information about it, or express any opinion about Montessori & Me, unless they are specifically authorised to do this.
- Befriend any clientele of Montessori & Me on any social media sites.

- Send unprotected sensitive or confidential information externally.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of the settings manager
- Connect Montessori & Me devices to the internet using non-standard connections.

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, Montessori & Me enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using a shredder.

Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Equipment and media taken off-site must not be left unattended at home, in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places).
- Laptop encryption must be used.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only Montessori & Me authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

Software

Employees must use only software that is authorised by Montessori & Me on the settings devices. Authorised software must be used in accordance with the software supplier's licensing agreements.

Individuals must not:

Store personal files such as music, video, photographs or games on the settings IT equipment

Viruses

Montessori & Me manager has implemented centralised, automated virus detection and virus software updates within the setting. All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

- Remove or disable anti-virus software

- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved setting anti-virus software and procedures.

Access to staff personal data

Employees are allowed to have access to all personal data about them held on manual or computer records under the Data Protection Act (1998). The Act requires the organisation to action requests for access to personal data within one month.
Should an employee request access to their personal data, the request must be addressed in writing to the relevant line manager. The request will be judged in the light of the nature of the personal data and the frequency with which they are updated. The employee will be informed whether or not the request is to be granted. If it is, the information will be provided within one month of the date of the request.
In the event of a disagreement between an employee and the line manager regarding personal data, the matter should be taken up under the settings grievance procedure.
The right of employees to see information held about them is extended to information held in paper record-keeping systems as well as computerised systems.
There are some exemptions; for example employees will not be able to see employment references about them supplied in confidence, nor will people involved in negotiations with the data controller be able to see information about the data controller's intentions in relation to those negotiations.

Legal Framework

General Data Protection Regulation 2018
https://ico.org.uk/ Data Protection Act 1998
Computer Misuse Act 1990
Freedom of Information Act 2000
Human Rights Act 1999
The Children Act 2004, 2006 (Every Child Matters) Statutory Framework Statutory Framework for the Early Years Section 3: The Safeguarding and Welfare requirements 3.67-3.72 Guidance
Please see separate Safeguarding Children Policy

This policy was adopted on 20/05/2018 Date for review: May 2019

Signed on behalf of the nursery: