GENERAL DATA PROTECTION REGULATION POLICY

GDPR stands for General Data Protection Regulation this replaces the previous Data Protection Policy Directives that were in place. GDPR is an EU directive regarding data protection and management.

It becomes enforceable from 25th May 2018 and will replace the previous directives.

GDPR aims primarily to give increased control to the public over their personal data.

Data Protection allows individuals to know what information is being held about them and have access to it if they wish.

Emmer Green Pre-school needs to keep certain information relating to staff, trustees, committee members, parents and children that have any interaction with the pre-school.

GDPR states that personal data shall be ‘processed fairly and lawfully’ and collected for specified, explicit and legitimate purposes’.

Sharing of Data

Emmer Green Pre-school holds data in order to comply with the EYFS Statutory Framework and is sometimes required to pass on information to the following organisations:

* Local Authorities (LA’s)
* Ofsted
* DFE

Children’s Files

Emmer Green Pre-school holds information on children to:

* Support their development
* Monitor their progress
* Provide appropriate care
* Assess how well the setting itself is doing
* Apply for funding

The information we hold includes contact details, date of birth, attendance information, special educational needs, any relevant medical information, accident reports, any files relating to safeguarding. Parent/carer data supplied will also be kept on record by the setting.

All paper copies of children’s files are kept in a locked cabinet in the office. Members of staff can have access to these files during the daytime but the cabinet and the office is locked at the end of each day. Any old children’s files are kept onsite and locked away. These records are shredded after the retention period.

When a child start’s at the pre-school the parent is asked to sign a declaration which is incorporated into the Confidential Details Admissions Form. It states in there what we will use the information for and to whom we may pass the information on to.

Photographs

We take photographs of the children to complete their Learning Journeys. All cameras are locked away at the end of each day and weekly all pictures are deleted from them. There will be no children’s pictures displayed anywhere without the consent of the parent.

Staff Data

We keep all staff files locked away in a filing cabinet only accessed by the Supervisor and Administrator. We ask that all staff sign a declaration to state that they are happy for us to keep relevant details about them.

We keep the files for the minimum amount of time that is required once that member of staff has left and this is (seven years). After this time the information in the file will be securely destroyed.

Trustees/Committee Data

Any information we hold relating to Trustees/Committee members is locked away in a secure cabinet. The only information that we publish relating to these positions is on the Charities Commission website and we always obtain permission before we publish this. This is a requirement of the Charities Commission to have this information listed. Any Trustees/Committee are asked to sign a declaration form. Information we hold is only retained for the minimum period and is securely destroyed afterwards.

Encryption

All files should be stored on encrypted memory sticks that allow a password to access them. Only the Administrator, Supervisor and Deputy will use these sticks to access files.

If sending personal data about staff and children via emails the information should be placed in a file and attached. The file should be password protected.

If you are sending hard copies of data to anyone either deliver it in person (where possible) or send it as recorded mail, so you know who has signed and received them.

If you are sending emails, please be mindful that you should not publish other people’s email addresses.

Working Off-site

There are times when staff will use laptops off site and any mobile devices. Equipment and media taken off site must not be left unattended in public places and not left in a car.

Care should be taken with laptops and mobile data, and all should be encrypted with a password.

Any Learning Journey’s that are taken home to work on must be taken in a locked case and not left unattended at any time.

Right of Access

If a member of staff or parent/carer would like access to a file, we request that we receive a written request to the Supervisor/Administrator. We will try and deal with that request within one month from the date of the letter. Please be aware there may be a charge if the information required takes a lot of investigating.

Reporting a Security Breach

We are a member of the Information Commissioner’s Office (ICO). The ICO is the UK’s independent body setup to uphold information rights. If there is a breach of security it should be reported to the Supervisor or Administrator in the first instance and then the breach must be reported to the ICO within 72 hours. The person/people concerned will be informed as soon as possible.

Policy adopted by the pre-school on ....................................................................................

Signed on behalf of the committee .......................................................................................

Name of Signatory (Full Name and Position) .........................................................................