**SECTION 2**
**General Data Protection Regulation (GDPR)/ Confidentiality**

**Policy Statement**

It is our intention to respect the privacy of children and their parents and carers, while ensuring that they access high quality nursery care and education. We ensure that all parents, carers and staff, can share their information in the confidence that it will only be used to enhance the welfare of their children

**2.1 GDPR requirements**

On the 25th May 2018 the General Data Protection Regulation (GDPR) will become law and replaces the Data Protection Act. It sets out requirements for those who have responsibility for data protection and we are already introducing this in to our procedures. There are 12 steps that need to be followed:

1. **Awareness**
2. **Information we hold**
3. **Communication privacy**
4. **Individuals rights**
5. **Subject access records**
6. **Lawful basis for processing personal data**
7. **Consent**
8. **Children**
9. **Data breaches**
10. **Data Protection by Design and Data Protection Impact Assessments**
11. **Data protections officers**
12. **International**
13. **Awareness**

All staff are aware of GDPR law and that it is replacing the Data Protection Act. Personal data is any data that can be linked to a single person and which identifies them in some way. The new GDPR regulations require us to let everyone know what data we hold on them, and that it has been agreed that we can hold the data, how we store it, who we might share it with (if anyone) and how long we keep the data on file for. We have discussed this at office meetings and advised staff of the impact it will have on them, they are aware that we are implementing the new procedures in to our setting and regular training and updates are given to staff. There are new obligations regarding personal data and new rights for individuals. Reviewing our GDPR gives us the opportunity to establish strong, secure data protection procedures. If any personal data is lost, destroyed or unwittingly shared it is our responsibility to report this breach to the Information Commissioners Office (ICO). All senior managers are responsible for implementing GDPR procedures. The manager, Rachel Austin and the admin assistant Claire Holdgate, oversee the introduction and monitoring of GDPR and a data audit is held annually and any changes made are recorded

1. **Information we hold**

Our privacy notice details the personal data we hold, where it came from and who we share it with. This is given to all parents/carers in the starter pack when a child starts the setting and they must be signed by parent/carer. We have a separate privacy notice and consent form for staff and contractors which is given to them on the first day of employment. Our social media, photo usage and Tapestry (our online journal) procedures are also explained in this document. Should information be shared in error, we will be able to refer to our records so that this can be corrected. Essex County Council, NHS, and our online learning journal, Tapestry have an extensive GDPR policy outlining their data protection rules and regulations to which we adhere to. For any private professionals arranged by the parent or carer, we would ask that they provide us with their relevant privacy notice.

We are obliged to share confidential information without authorisation from the person who provided it or whom relates if it is in the public interest. That is when:

* It is to prevent a crime from being committed or intervene where one may have been or to prevent harm to a child or adult; or
* Not sharing it could be worse than the outcome of having shared it.
* The decision should never be made as an individual, but with the backup of management committee officers. The three criteria are:
	+ Where there is evidence that the child is suffering, or is at risk of suffering, significant harm.
	+ Where there is reasonable cause to believe that a child may be suffering or is at risk from suffering significant harm.
	+ To prevent significant harm to children and young people or serious harm to adults, including the prevention, detection and prosecution of serious crime.
1. **Communicating privacy**

Our lawful basis for processing this data is to ensure that your child is entitled to a place at the setting and that the nursery receives the statutory funding from the government that it is entitled to, we ask for your consent to retrieving and subsequently recording this information in the consent section at the end of the terms and conditions document. For staff, our lawful basis for processing data is to ensure that you are eligible to work in the UK and that you are safe to work with children.
We have a password protected database which is used to record when data on a child can be destroyed or deleted, it includes information such as date of birth, start date and leave date. We also hold hard copies of each child; all registration documents, any personal notes, external professional notes, we retain this information as we provide childcare for returning children up to the age of 8 years old (up to the day of their 8th birthday). We do have many returning children in the school holidays. For this reason we retain all children’s records until their 9th birthday. At this point, all information is destroyed, but for child protection purposes, accident/incident forms (including any shared information regarding a child’s health and wellbeing) (electronic and hard copy) are kept for 21 years or in the case of a child who is on the child protection register, the records will be kept for 24 years. All creative work is given to the parent or carer on their last day, all developmental and observational records uploaded to Tapestry, our online developmental tracking system, are saved as a PDF which is emailed to the parent, we then remove this from our Tapestry application within one month of the child leaving (in the event of a child who is on the child protection register, we would back up the data to our computer system and it would be retained with the accident and incident forms for 24 years).

We also have copies of our Public Liability Insurance certificates.

Electronic documents include Word, PDF and Excel. Deletion processes involve shredding of all hard copy paperwork and full deletion of records within the electronic database. Strong passwords (using lower case, upper case and numbers) are used on all personal or sensitive data.

All confidential information about a child will be sent via Egress, a highly secure encrypted software that delivers information electronically

All laptops, tablets and iPads are have antivirus software and firewall installed and this is automatically renewed.

Dropbox is used to store all our work on the laptops and iPads, this is a secure cloud based service for storing and sharing documents, it backs up our work so that we can retrieve it should we need to.

If you are not happy with our data handling procedures, we would ask you to contact us in the first instance, so that we may have the opportunity to resolve any issues. However, you have the right to complain further to the Information Commissioners Office (ICO) if you think there is a problem with the way we are handling the data.

1. **Individuals rights and 5. Subject access records**

In accordance to the GDPR we respect the rights of individuals. All staff has the right to view their own records. Every parent has the right to view their child’s folder and records that we hold on that child, we will do this within one month of asking and make no charge for this service. Parents/carers are not allowed to have access to any other child’s records. When a parent/staff member requests access to information there are several steps that must be taken, these are outlined in our privacy notice. Should a parent/staff member ask us to delete information, we will view the information and where we feel we must fulfil our safeguarding duty, we would make a managerial decision on how this would affect the child/staff member and if necessary we would seek advice from Children’s and families hub or OFSTED. We consider this to be ….

* It is to prevent a crime from being committed or intervene where one may have been or to prevent harm to a child or adult; or
* Not sharing it could be worse than the outcome of having shared it.
* The decision should never be made as an individual, but with the backup of management committee officers. The three criteria are:
	+ Where there is evidence that the child is suffering, or is at risk of suffering, significant harm.
	+ Where there is reasonable cause to believe that a child may be suffering or is at risk from suffering significant harm.
	+ To prevent significant harm to children and young people or serious harm to adults, including the prevention, detection and prosecution of serious crime.

Our procedure for sharing information is based on the 6 points of good practice as set out in information sharing practitioners guide (HM Guidance 2015)

1. Explain to families how, when and why information will be shared about them and with whom. That consent is normally obtained, unless it puts the child at risk, or undermines criminal investigation.

* We ensure parents receive information about our information sharing policy when starting their child in the setting and they sign the form to say that they understand circumstances when information may be shared without their consent. This will only be when it is a matter of safeguarding a child or vulnerable adult.
* We ensure parents have information about safeguarding children.
* We ensure parents have information about circumstances when information will be shared with external agencies for example with regard to any special needs the child may have or transition to school.

2. Consider the safety and welfare of the child when making a decision and sharing information- if there are concerns regarding ‘significant harm’ the child’s well-being and safety is paramount.

* We record concerns and discuss these with the settings designated person. Record decisions made and the reasons why information will be shared and with whom.
* We follow the procedures for reporting concerns and record keeping.

3. Respect the wishes of children and parents not to consent to share confidential information. However, in the interests of the child, we are able to judge when it is reasonable to override their wish.

* Guidelines for consent are part of this procedure.
* Managers are conversant with this and are able to advise staff accordingly.

4. Seek advice when there are doubts about possible significant harm to a child or others.

* Managers contact Childrens and Families Hub for advice when they have doubts or are unsure.

5. Information shared should be accurate and up-to-date, necessary for the purpose it is being shared for and shared only with those who need to know and shared securely.

* Our safeguarding children and child protection procedures and record keeping procedures set out how and where information should be recorded and what information should be shared with another agency when making a referral.

6. Reasons for decisions to share information, or not are recorded

**6. Lawful basis for processing personal data**
We require the information to ensure that your child is entitled to a place at the setting and that the setting receives the statutory funding which it is eligible for and so that we are able to provide the relevant care and education for that child. For staff, it is to ensure that you they are eligible to work in the UK and are safe to work with children. Our website is for information purposes only, we do not ask you to log in, nor do we ask for any personal information, so we do not have any form of recording your data or your browsing, so we therefore do not have a cookies requirement.

**7. Consent**
Consent within our setting is of the highest priority. Before a child starts parents are sent our privacy notice and consent form and policies and procedures to which the parent signs and consents and returns a copy to the nursery. Staff members are also given the same staff relevant paperwork Consent is ongoing within our nursery as we require permission continually throughout the year. You are able to retract your consent any time, procedures for this are as set out in our privacy notice. The new GDPR regulations do not prohibit the sharing of information if there are child safeguarding concerns. In accordance to the ICO terms and conditions on ‘Consent’, we have a lawful basis to share information without your prior consent, under the lawful basis ‘vital interest’ rule where we feel that processing that data is necessary to protect someone’s life.

1. **Children**

Birth certificates are seen in order to verify a child’s age. If we require further information other than the birth certificate (or are dissatisfied about the birth certificate given), we would contact Children’s and families hub. Parental permission and consent is given on many subjects relating to the data processing activity of children’s records, detailed information is within our privacy notice in the terms and conditions document.

1. **Data breaches**

We have procedures in place in the unlikely event of a data breach, either access to electronic files or hard copy files.

* If a child’s records have been accessed in error, the parent or carer of the individual would be notified immediately
* For any information unwittingly emailed to the wrong email address, we would contact the recipient and ask that they delete the email, without reading its content
* If an email about a child has been received by a person in error, unaware to the nursery, we would ask that they contact us immediately and delete the email without reading its content
* If staff details have been breached the staff member would be alerted
* If we become aware that there had been unauthorised access to records within the building, we would notify all parents and staff immediately
* We would check the folders for every single child and staff member ensuring that all the information is still within the folder
* Any data breach would be recorded
* We would evaluate our procedures for recording and sharing data
* We would also contact the Information Commissioners Office (ICO) who are responsible for the GDPR and OFSTED. In some circumstances, we would notify the police and social services.
* We do not ask for nor record bank details for parents or children
1. **Data Protection by Design and Data Protection Impact Assessments**

Our approach is to assess and evaluate all the work that we do in terms of the impact it may have on data protection. As a nursery, we do not have a need for software or apps that record or control our data, neither do we process data on a large scale. We aim to identify problems at an early stage to minimise any negative effect they may have. We are governed by many legislations and this has to be incorporated in to the day to day practice within the nursery. When evaluating our policies and procedures we examine and make careful notes on any new law that has been implemented and we do this continually as new updates are constantly received by OFSTED, NDNA and Essex County Council.

1. **Data protection officers**

All senior managers are responsible for implementing GDPR procedures. The manager, Rachel Austin and the admin assistant Claire Holdgate, oversee the introduction and monitoring of GDPR.

1. **International**

We are an independent company and with one setting in Brentwood, Essex, UK. International GDPR is not relevant to our setting

This policy has been reviewed and updated by Rachel Austin and Claire Holdgate on 8th January 2019. It has also had the input from all staff members and approved by them.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_