



Policy on Confidentiality

We will meet the EYFS requirements by:

- Developing a professional relationship with all parents and/or carers; treating information shared with us as confidential (unless this compromises a child's safety or welfare, in which case The Nursery will be required to disclose sensitive and confidential information to appropriate agencies).
- Holding confidential information and records about children and assistants in a secure place; and only be accessible and available to those who have a right or a professional need to see them. (3.70)
- Complying with our responsibilities under the Data Protection Act (DPA) 2018 & GDPR 2016 and where relevant the Freedom of Information Act 2000. (3.78)

During the day, the Nursery's staff will encounter confidential information. To ensure that all those using and working in the nursery can do so with confidence, we will respect confidentiality in the following ways:

The nursery manager ensures that all staff members are aware of the need to maintain privacy and confidentiality through induction training. All members of staff and students will have this policy explained to them and will be expected to sign to say they agree to it. All information kept on children will only be shared with the parents/carers, key worker and Nursery Manager. Permission is sought from Parents/carers for staff to share records with outside agencies for example, Health Visitor or the Early Years Team. In addition, parents can have access to their child's records at any time, provided there no relevant exemptions apply under the General Data Protection Regulation (GDPR).

Staff will not discuss any child with anyone other than the child's parents/carers. We will consider the need for confidentiality when having discussions with other adults and ask that other parents/carers acknowledge and respect our need for discretion. All information relating to individual children will be stored securely on the nursery computer, for example, in password protected files.

The nursery uses Eylog for the children's electronic learning journeys and Eymanage as a management software program. Both of these systems are password protected and can only be accessed by authorised staff. Parents must agree to not share photographs or videos from their child's electronic learning journey on social media that contain images of children other than their own. When a child leaves the setting, they will be made 'inactive' and removed from all platforms (in line with 'storage limitation' within the GDPR). Staff who have left the setting will be made 'inactive' and removed so they are unable to access any personal details.



Data Protection (including Confidentiality) Policy

At Fledglings, we recognise that we hold sensitive and confidential information about children and their families and the staff we employ. This information is used to meet children's needs, for registers, invoices and emergency contacts. We store all records in a locked cabinet or on the office computer with files that are password protected in line with data protection principles. Any information shared with the staff team is done on a 'need to know' basis and treated in confidence. This policy works alongside the GDPR privacy notice to ensure compliance under General Data Protection Regulation (Regulation (EU) 2016/679 (GDPR) and Data Protection Act 2018.

Legal requirements

- We follow the legal requirements set out in the Statutory Framework for the Early Years Foundation Stage (EYFS) 2021 and accompanying regulations about the information we must hold about registered children and their families and the staff working at the nursery.
- We follow the requirements of the General Data Protection Regulation (Regulation (EU) 2016/679 (GDPR), Data Protection Act 2018 and the Freedom of Information Act 2000 with regard to the storage of data and access to it.

Procedures

It is our intention to respect the privacy of children and their families and we do so by:

- Storing confidential records in a locked filing cabinet or on the office computer with files that are password protected
- Ensuring staff, student and volunteer inductions include an awareness of the importance of the need to protect the privacy of the children in their care as well as the legal requirements that exist to ensure that information relating to the child is handled in a way that ensures confidentiality. This includes ensuring that information about the child and family is not shared outside of the nursery other than with relevant professionals who need to know that information. It is not shared with friends and family, or part of any social discussions outside of the setting. If staff breach any confidentiality provisions, this may result in disciplinary action and, in serious cases, dismissal. Students on placement in the nursery are advised of our Data protection and confidentiality policy and required to respect it.
- Ensuring that all staff, volunteers and students are aware that information about children and families is confidential and only for use within the nursery and to support the child's best interests with parental permission.

- Ensuring that parents have access to files and records of their own children but not to those of any other child, other than where relevant professionals such as the police or local authority children's social care team decide this is not in the child's best interest
- Ensuring all staff are aware that this information is confidential and only for use within the nursery setting. If any of this information is requested for whatever reason, the parent's permission will always be sought other than in the safeguarding circumstances above
- Ensuring staff do not discuss personal information given by parents with other members of staff, except where it affects planning for the child's needs
- Ensuring staff, students and volunteers are aware of and follow our Social networking policy in relation to confidentiality
- Ensuring issues concerning the employment of staff remain confidential to the people directly involved with making personnel decisions
- Ensuring any concerns or evidence relating to a child's personal safety are kept in a secure, confidential file and are shared with as few people as possible on a 'need-to-know' basis. If, however, a child is considered at risk, our Safeguarding children and child protection policy will override confidentiality.

All the undertakings above are subject to the paramount commitment of the nursery, which is to the safety and well-being of the child.

General Data Protection Regulation (Regulation (EU) 2016/679 (GDPR) compliance

In order to meet our requirements under GDPR we will also undertake the following:

- We will ensure our terms and conditions, privacy and consent notices are easily accessed and made available in accurate and easy to understand language
- We will use personal data to ensure the safe, operational and regulatory requirements of running our nursery. We will only make contact in relation to the safe, operational and regulatory requirements of running our nursery, these include. We will not share or use personal data for other purposes. Further detail can be found in the GDPR privacy notice
- Everyone in our nursery understands that people have the right to access their records or have their records amended or deleted (subject to other laws and regulations)
- We will ensure staff have due regard to the relevant data protection principles, which allow them to share (and withhold) personal information, as provided for in the Data Protection Act 2018 and the GDPR. This includes:
 - Being confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information which is sensitive and personal, and should be treated as 'special category personal data'
 - Understanding that 'safeguarding of children and individuals at risk' is a processing condition that allows practitioners to share special category personal data. This

includes allowing practitioners to share information without consent where there is good reason to do so, and that the sharing of information will enhance the safeguarding of a child in a timely manner, but it is not possible to gain consent, it cannot be reasonably expected that a practitioner gains consent, or if to gain consent would place a child at risk.

Staff and volunteer information

- All information and records relating to staff and volunteers will be kept confidentially in a locked cabinet or through password protected files stored online (one drive/BrightHR/Eymanage systems)
- Individual staff may request to see their own personal file at any time.