

4.4 Confidentiality and client access to records policy

Policy statement

'Share with informed consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, there is good reason to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case.'

Information sharing: Advice for practitioners providing safeguarding services to children, young people, parents, and carers (HMG 2015)

At Perins Pre-School, we recognise that we hold sensitive/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 cupboard or on the office computer which is 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 will work alongside the 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 setting.
- 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 regarding 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 confidentiality and that information about the child and family is not shared outside of the setting other than with relevant professionals who need to know that information. It is not shared with friends and family, or part of any social discussion 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 setting are advised of our confidentiality policy and required to respect it
- Ensuring that all staff, volunteers, and students are aware that this information 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 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/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/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

To meet our requirements under GDPR we will also undertake the following:

1. We will ensure our terms & conditions, privacy and consent notices are easily accessed/made available in accurate and easy to understand language.
2. We will use your data to ensure the safe, operational, and regulatory running of our setting. We will only contact you in relation to the safe, operational running of the setting. We will not share or use your data for other purposes.
3. Everyone in our setting understands that people have the right to access their records or have their records amended or deleted (subject to other laws and regulations).

Client access to records procedures

Parents may request access to any confidential records we hold on to their child and family following the procedure below:

- The parent is the 'subject' of the file in the case where a child is too young to give 'informed consent' and has a right to see information that our setting has compiled on them.
- Any request to see the child's personal file by a parent or person with parental responsibility must be made in writing to the manager.
- We acknowledge the request in writing, informing the parent that an arrangement will be made for him/her to see the file contents, subject to third party consent.
- Our written acknowledgement allows one month for the file to be made ready and available. We will be able to extend this by a further two months where requests are complex or numerous. If this is the case, we will inform you within one month of the receipt of the request and explain why the extension is necessary.
- A fee may be charged for repeated requests, or where a request requires excessive administration to fulfil.
- Our manager informs their line manager and the data and IT manager of Perins, and legal advice may be sought before sharing a file.
- Our manager goes through the file with their line manager and the data and IT manager and ensures that all documents have been filed correctly, that entries are in date order and that there are no missing pages. They note any information, entry or correspondence or other document which mentions a third party.
- We write to each of those individuals explaining that the subject has requested sight of the file, which contains a reference to them, stating what this is.
- They are asked to reply in writing to our manager giving or refusing consent for disclosure of that material.
- We keep copies of these letters and their replies on the child's file.
- 'Third parties' include each family member noted on the file; so, where there are separate entries pertaining to each parent, stepparent, grandparent etc. we write to each of them to request third party consent.
- Third parties also include workers from any other agency, including children's social care and the health authority for example. Agencies will normally refuse consent to share information, preferring instead for the parent to be redirected to those agencies for a request to see their file held by that agency.
- Members of staff should also be written to, but we reserve the right under the legislation to override a refusal for consent or to just delete the name of the staff member and not the information. We may grant refusal if the member of staff has provided information that could be considered 'sensitive' and the staff member may be in danger if that information is disclosed; or if that information is the basis of a police investigation. However, if the information is not sensitive, then it is not in our interest to withhold that information from a parent. In each case this should be discussed with members of staff and decisions recorded.
- When we have received all the consents/refusals, our manager takes a photocopy of the complete file. On the copy of the file, our manager removes any information that a third party has refused consent for us to disclose and blank out any references to the third party, and any information they have added to the file, using a thick marker pen.

- The line manager and legal advisors, verify that the file has been prepared appropriately then check the copy file.
- What remains is the information recorded by the setting, detailing the work initiated and followed by them in relation to confidential matters. This is called the 'clean copy'.
- We photocopy the 'clean copy' again and collate it for the parent to see.
- Our manager informs the parent that the file is now ready and invite[s] him/ her to make an appointment to view it.
- Our manager and their line manager meet with the parent to go through the file, explaining the process as well as what the content of the file records about the child and the work that has been done. Only the person(s) with parental responsibility can attend that meeting, or the parent's legal representative or interpreter.
- The parent may take a copy of the prepared file; but to ensure it is properly explained to and understood by the parent, we never hand it over without discussion.
- It is an offence to remove material that is controversial or to rewrite records to make them more acceptable. Our recording procedures and guidelines ensure that the material reflects an accurate and non-judgemental account of the work we have done with the family.
- If parents feel aggrieved about any entry in the file, or the resulting outcome, then we refer the parent to our complaint's procedure.
- The law requires that the information we hold must be held for a legitimate reason and must be accurate (see our Privacy Notice). If a parent says that the information, we hold is inaccurate, then the parent has a right to request for it to be changed. However, this only pertains to factual inaccuracies. Where the disputed entry is a matter of opinion, professional judgement, or represents a different view of the matter than that held by the parent, we retain the right not to change that entry, but we can record the parent's view of the matter. In most cases, we would have given a parent the opportunity at the time to state their side of the matter, and it would have been recorded there and then.
- If there are any controversial aspects of the content of a child's file, we must seek legal advice. This might be where there is a court case between parents, where social care or the police may be considering legal action, or where a case has already completed, and an appeal process is underway.
- We never 'under-record' for fear of the parent seeing, nor do we make 'personal notes' elsewhere.

Telephone advice regarding general queries may be made to The Information Commissioner's Office Helpline 0303 123 1113.

All the undertakings above are subject to the paramount commitment of our setting, which is to the safety and well-being of the child. Please see also our policy on Safeguarding Children and Child Protection.

Record Retention

This policy is subject to the laws relating to data protection and document retention. We are required under legislation to keep certain records about children, parents/carers, and staff members. Due to this legislation, we are required to keep this information for a set amount of time.

- Children's records - A reasonable period after children have left the provision.
- Records relating to individual children (care plans, referral forms) – We will pass these on to the child's next school or setting. Copies will be kept for a period.
- Accident and pre-existing injuries - If relevant to child protection, we will keep these until the child reaches 25 years old.
- Safeguarding records and cause for concern form – We will pass these onto the child's new school or setting. If we are not informed of the child's new placement, we will keep the records until the child reaches 25 years old.
- Records of any reportable death, injury, disease, or dangerous occurrence (for the children) – As these incidents could result in potential negligence claims, or evolve into more serious health condition, we keep records until the child reaches the age of 21 years and 3 months.
- Records of any reportable death, injury, disease, or dangerous occurrence (for staff) – 3 years
- Types of accidents include fractures, broken limbs, serious head injuries, or where the child is hospitalised – until the child reaches the age of 21 years and 3 months.
- Personnel files and training records – 7 years
- Visitors signing book – up to 24 years as part of the child protection trail.

Legal framework

- General Data Protection Regulations (GDPR) (2018)
- Human Rights Act (1998)

Further guidance

- Information sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers (HM Government 2015)

This policy was adopted by

Perins Pre-school

On

25th April 2023

Date to be reviewed

25th April 2024

Signed on behalf of the provider

Michelle Osman

Name of signatory

Michelle Osman

Role of signatory (e.g. chair, director or owner)

Pre-School Manager