St. James' Church
Rowledge
Farnham
GU10 4EN
01252 794617
manager@littlefishesrowledge.org.uk
admin@littlefishesrowledge.org.uk

07 LF Records & Data Protection Policy and Procedures 25.26

Alongside procedures in 07.01 – 07.04 this policy was adopted by Little Fishes on 31/01/23 and reviewed on 11/01/24& 04/04/25. Latest changes made are shown in red.

Next review date: January 2026

Data Controllers	St James Church	
Data Processer	Little Fishes Nursery School	Church Lane, Rowledge, Farnham, GU10 4EN
Data Protection Lead	Rev Dr Stephen Green: Vicar of St. James church	vicar@stjamesrowledge.org.uk 01252 792402
Data Protection Administrator	Emily Scotcher	admin@littlefishesrowledge.org.uk 01252 794617

Contents:

07 Record Keeping and Data Protection Policy

Aim

We have record keeping systems in place for the safe and efficient management of the setting and to meet the needs of the children. They meet the legal requirements for the storing and sharing of information within the framework of the GDPR and Data Protection Act 2018 and the Human Rights Act 1998.

Record Keeping Objectives

- There is a procedure for recording general information about children's development and learning, welfare and safeguarding and child protection concerns.
- Children's development and learning records are kept in personal folders, either in paper folders or in their online learning journal on Tapestry.
- Children's registration, funding, finance and welfare records are kept in securely in either digital or paper folders and divided into appropriate sections and stored separately from their development records.
- Information on child attendance, hours, staff present, and outings are kept in Tapestry, our digital learning journal and management system.
- Some details such as key persons, emergency contact details, medical and health, are also kept physically in the register.
- Records of a more confidential nature are stored in children's personal files, as required, such as Common Assessment Framework assessments, Early Support information or Education, Health and Care Plan (EHCP), discussions with parents, and action taken, copies of correspondence and reports from other agencies or are stored digitally, with secure cloud-based storage (Microsoft Sharepoint).
- Materials and records relating to safeguarding and child protection, such as case notes, including recording of concerns and safeguarding concerns, are kept in a separate safeguarding file, with restricted access
- Ethnicity data is only recorded where parents have identified the ethnicity of their child themselves.
- Confidentiality is maintained by secure storage of files in a locked cabinet with access restricted to those who need to know. All digital files are stored securely, with restricted access, and access is password protected.
- Client access to records is provided for within this policy, section 07.03 Client access to records.
- Staff know how and when to share information **effectively** if they believe a family may require a particular service to achieve positive outcomes and promote the welfare of the children. This includes sharing information that is **relevant, adequate, and accurate.**
- Staff know how to share information, in a **timely and secure** manner, if they believe a child is in need or at risk of suffering harm.
- Staff understand 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'
- If the individual can be identified from the information that has been shared, staff record when and to whom information has been shared, why information was shared and whether consent was given. Where consent has not been given and staff have taken the decision, in line with guidelines, to override the refusal for consent, the decision to do so is recorded.

- Guidance and training for staff specifically covers the sharing of information between professions, organisations, and agencies as well as within them, and arrangements for training takes account of the value of multi-agency as well as single agency working.

Types of records and documentation held:

The following information and records are held in line with *07.01a LF families privacy notice* and *07.01b LF staff privacy notice*:

- Name, address and contact details of the provider and all staff employed on the premises
- Name address and contact details of any other person who will regularly be in unsupervised contact with children
- A daily record of all children looked after on the premises, their hours of attendance and their named key person
- Certificate of registration and named person responsible for setting
- Children's personal information, including full name, date of birth, health, welfare and development records
- Name and address of every parent and/or carer known to our setting and information about any other person who has parental responsibility for the child, who the child normally lives with
- Parent and / or carer emergency contact information (see families privacy notice)
- Certificate of registration, ICO registration and insurance document are all displayed and shown to parents on request
- Records of risk assessments
- Record of complaints
- Record of incidents
- Staff training, supervision, appraisal, and other information

Principles of data protection and safeguarding recording

Lawful processing of data

Personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is not compatible for these purposes
- adequate, relevant and necessary in relation to the purposes for which they are processed
- accurate, and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purpose for which they are processed, are erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality") Article 5 of the General Data Protection Regulations (2018)

Little Fishes Nursery School processes data and records and shares information in line with the principles above.

General safeguarding recording principles

- It is vital that all relevant interactions linked to safeguarding children's and individual's welfare are accurately recorded.
- All recordings should be made as soon as possible after the event.
- Recording should be to a good standard and clear enough to enable someone other than the person who wrote it, to fully understand what is being described.
- Recording can potentially be viewed by a parent/carer or Ofsted inspector, by the successors of the practitioners who record, and may be used in a family Court as relevant evidence to decide whether a child should remain with their biological parents or be removed to live somewhere else. Recording needs to be fair and accurate, non-judgemental in tone, descriptive, relevant, and should clearly show what action has been taken to safeguard a child and, reflect decision-making relating to safeguarding.
- Recording should be complete, it should show what the outcome has been, what happened to referrals, why decisions were made to share or not share information, and it should contain summaries and minutes of relevant multi-agency meetings and multi-agency communication.
- If injuries or other safeguarding concerns are being described the description must be clear and accurate and should give specific details of the injury observed and where it is located.

The principles of GDPR and effective safeguarding recording practice are upheld

- Recording is factual and non-judgemental.
- The procedure for retaining and archiving personal data and the retention schedule and subsequent destruction of data is adhered to.
- Parents/carers and children where appropriate are made aware of what will be recorded and in what circumstances information is shared, prior to their child starting at the setting. Parents/carers are issued with the Families Privacy Notice and must give signed, informed consent to recording and information sharing prior to their child attending the setting. If a parent/carer would not expect their information to be shared in any given situation, normally, they should be asked for consent prior to sharing.
- There are circumstances where information is shared without consent to safeguard children. These are detailed below, but in summary, information can be shared without consent if a practitioner is unable to gain consent, cannot reasonably be expected to gain consent, or gaining consent places a child at risk. Records can be accessed by, and information may be shared with, local authority professionals. If there are significant safeguarding or welfare concerns, information may also be shared with a family proceedings Court or the police. Practitioners are aware of information sharing processes and all families should give informed consent to the way the setting will use, store and share information. Recording should be completed as soon as possible, and within 5 working days as a maximum for safeguarding recording timescales.

- If a child attends more than one setting, a two-way flow of information is established between the parents/carers, and other providers. Where appropriate, comments from others (as above) are incorporated into the child's records.

07.01 PROCEDURE: Children's records and recording information

Children's personal records

The contents of children's personal records are kept in line with our procedures (*07.01 Keeping Children's personal records*), with access restricted as appropriate.

- Children's paper personal files and information are kept in a filing cabinet, which is always locked when not in use, or digitally on a secure server, or on an online learning management platform. The location of children's records are listed in Appendix 1.
- Access to children's personal files and information is restricted to those authorised to see them and make entries in them, this being the setting manager, deputy or designated person for child protection, the child's key person, or to staff as authorised by the setting manager.
- Safeguarding records and information are kept in a filing cabinet, which has restricted access and which is always locked when not in use, or digitally on a secure server.
- Correspondence in relation to a child is read, any actions noted, and filed immediately
- Children's personal files are not handed over to anyone else to look at.
- Children's files may be handed to Ofsted as part of an inspection or investigation; they may also be handed to local authority staff conducting a S11 audit as long as authorisation is seen.

Procedure for recording children's information

- When recording general information, staff should ensure that records are dated correctly and the time is included, where necessary, and signed.
- Safeguarding /child protection concerns are recorded on an *06.01b Expression of Concern form* (see 06: Safeguarding Policy)
- It is important that members of staff explain to parents that sometimes it is necessary to write things down in their child's file and explain the reasons why.
- Information is clear and unambiguous (fact, not opinion), although it may include the practitioner's thoughts on the impact on the child.
- Records are non-judgemental and do not reflect any biased or discriminatory attitude
- Not everything needs to be recorded, but significant events, discussions and telephone conversations must be recorded at the time that they take place.
- Recording should be proportionate and necessary.
- When deciding what is relevant, the things that cause concern are recorded as well as the action taken to deal with the concern. The appropriate recording format is filed within the child's file.
- Where a decision is made to share information (or not), reasons are recorded. Note what is shared, date and by whom.

- Digital copies of reports are stored securely with Microsoft OneDrive.
- Staff may use a personal computer to type reports, or letters. Where this is the case, staff access files with Microsoft OneDrive/SharePoint our password protected internet-based cloud storage platform. No documents are stored on the staff member's computer.
- With permission from the setting manager, a member of staff may use their personal phone to take high quality photos of an event e.g. nativity play. Where this is the case, photos are downloaded and stored on a secure internet-based cloud storage platform (iPhoto or OneDrive) and deleted from the personal phone within 48 hours of the event.

Recording absences and outbreak management

- All absences are recorded on the Tapestry register, recording; child's name, reason for absence, when they are expected to return, method of contact and staff reporting.
- Absences are tracked as part of our outbreak management. Illnesses and diseases that are notifiable or require management are specifically recorded using a colour key.
- During a notifiable outbreak of an illness or disease there may be the need to keep additional records as part of outbreak management.
- Additionally, a record of all confirmed cases of Covid-19 that affect any member of staff or child is held. A record is kept of individual cases of children who are self-isolating due to symptoms as per usual record-keeping procedures. In all cases the principles of data protection are maintained.

07.02 PROCEDURE: Confidentiality and sharing information

Confidentiality

The definition of confidentiality is: Personal information of a private or sensitive nature, which is not already lawfully in the public domain or readily available from another public source, and has been shared in a relationship, where the person giving the information could reasonably expect it would not be shared with others.
Policies and procedures set out the responsibility of the setting regarding gaining consent to share information, and when it may not be sought or overridden.

- Staff can be said to have a 'confidential relationship' with families. Some families share information about themselves readily; members of staff need to check whether parents regard this information as confidential or not.
- Parents sometimes share information about themselves with other parents as well as staff; the setting cannot be held responsible if information is shared beyond those parents whom the person has confided in.
- Information shared between parents in a group is usually bound by a shared agreement that the information is confidential and not discussed outside. The setting manager is not responsible should that confidentiality be breached by participants.
- Where third parties share information about an individual; staff need to check if it is confidential, both in terms of the party sharing the information and of the person whom the information concerns.

- Information shared is confidential to the setting.
- Practitioners ensure that parents/carers understand that information given confidentially will be shared appropriately within the setting (for instance with a designated person, during supervision) and should not agree to withhold information from the designated person or their line manager.

Most things that happen between the family, the child and the setting are confidential to the setting. In certain circumstances information is shared, for example, a child protection concern will be shared with other professionals including social care or the police, and settings will give information to children's social workers who undertake S17 or S47 investigations.

Personal information can be shared lawfully if it is to keep a child or individual safe from neglect, physical, emotional or mental harm or to protect their physical, mental or emotional wellbeing.

Normally parents should give informed consent before information is shared. Information can be shared legally, without consent if a practitioner is unable to or cannot reasonably expect to gain consent from an individual or if to do so may place a child at risk. If a serious offence may have been committed, parental consent should not be sought before information is shared.

Hampshire Safeguarding Children Partnership (HSCP) procedures should be followed when making referrals, and advice sought if there is a lack of clarity about whether parental consent is needed before making a referral due to safeguarding concerns.

Staff discuss children's general progress and well-being together in meetings, but more sensitive information is restricted to designated persons and key persons and shared with other staff on a need-to-know basis.

Members of staff do not discuss children with staff who are not involved in the child's care, nor with other parents or anyone else outside of the organisation, unless in a formal and lawful way.

See Appendix 2: Flow Chart of when and how to share information.

Sharing information with other professionals

- Discussions with other professionals should take place within a professional framework, not on an informal basis. Staff should expect that information shared with other professionals will be shared in some form with parent/carers and other professionals, unless there is a formalised agreement to the contrary, i.e. if a referral is made to children's social care, the identity of the referring agency and some of the details of the referral is likely to be shared with the parent/carer by children's social care.
- Information shared with other agencies is done in line with our procedures and where a decision is made to share information (or not), reasons are recorded.
- Staff may use a personal computer to type reports, or letters. Where this is the case, staff access and store files with secure internet-based cloud storage (Microsoft Onedrive/Sharepoint). No documents are stored on the staff member's computer.

- The setting is registered with the Information Commissioner's Office (ICO). The setting DP administrator can ensure that staff follow guidelines issued by the ICO, at https://ico.org.uk/for-organisations/
- Additional guidance in relation to information sharing about adults is given by the Social Care Institute for Excellence, at www.scie.org.uk/safeguarding/adults/practice/sharing-information
- Staff should follow guidance including Working Together to Safeguard Children (DfE 2023); Information Sharing: Advice for Practitioners Providing Safeguarding Services to Children, Young People, Parents and Carers 2024 and What to do if you're Worried a Child is Being Abused (HMG 2015)
- The setting manager and Data protection lead have regard to Keeping Children safe in education 2025 when sharing information

Breach of confidentiality

A personal data breach means: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. All members of staff should be vigilant and able to identify suspected personal data breach.
A breach could include:

- loss or theft of devices or data, including information stored on USB drives or on paper
- hacking or other forms of unauthorised access to a device, email account or the network
- disclosing personal data to the wrong person, through wrongly addressed emails, or bulk emails that inappropriately reveal all recipients' email addresses
- alteration or destruction of personal data without permission and not in line with policy.

A breach of confidentiality occurs when confidential information is not authorised by the person who provided it, or to whom it relates, without lawful reason to share. The impact is that it may put the person in danger, cause embarrassment or pain.

It is not a breach of confidentiality if information was provided on the basis that it would be shared with relevant people or organisations with lawful reason, such as to safeguard an individual at risk or in the public interest, or where there was consent to the sharing.

In the event of a breach:

- Where a member of staff discovers or suspects a personal data breach, this should be reported to the manager or Data Protection Administrator who will report to the Data Protection Lead (DPL) as soon as possible.
- DPL to immediately notify the Information Commission's Office (within 72 hours).
- In the event that full details of the nature and consequences of the data breach are not immediately accessible (e.g. because Data Processors do not work on every normal weekday), the DPL will bring that to the attention of the Information Commissioner's Office and undertake to forward the relevant information as soon as it becomes available. The Trustees will report the breach as a serious incident to the Charity Commission.
- Where there is likely high risk to individuals' rights and freedoms, Little Fishes will inform those individuals affected by the personal data breach without undue delay.

- The DPL will keep a record of all personal data breaches reported, and follow up with appropriate measures and improvements to reduce the risk of reoccurrence.

Exception

- GDPR enables information to be shared lawfully within a legal framework. The Data Protection Act 2018 balances the right of the person about whom the data is stored with the possible need to share information about them
- The Data Protection Act 2018 contains "safeguarding of children and individuals at risk" as a processing condition enabling "special category personal data" to be processed and to be shared. This allows practitioners to share without consent if it is not possible to gain consent, if consent cannot reasonably be gained, or if gaining consent would place a child at risk.
- Confidential information may be shared without authorisation - either from the person who provided it or to whom it relates, if it is in the public interest and it is not possible or reasonable to gain consent or if gaining consent would place a child or other person at risk. The Data Protection Act 2018 enables data to be shared to safeguard children and individuals at risk. Information may be shared to prevent a crime from being committed or to prevent harm to a child, Information can be shared without consent in the public interest if it is necessary to protect someone from harm, prevent or detect a crime, apprehend an offender, comply with a Court order or other legal obligation or in certain other circumstances where there is sufficient public interest.
- Sharing confidential information without consent is done only in circumstances where consideration is given to balancing the needs of the individual with the need to share information about them.
- When deciding if public interest should override a duty of confidence, consider the following:
    - is the intended disclosure appropriate to the relevant aim?
    - what is the vulnerability of those at risk?
    - is there another equally effective means of achieving the same aim?
    - is sharing necessary to prevent/detect crime and uphold the rights and freedoms of others?
    - is the disclosure necessary to protect other vulnerable people?

The decision to share information should not be made as an individual, but with the backing of the data protection lead who can provide support, and sometimes ensure protection, through appropriate structures and procedures.

Obtaining consent to share information

Consent to share information is not always needed. However, it remains best practice to engage with people to try to get their agreement to share where it is appropriate and safe to do so.

Using consent as the lawful basis to store information is only valid if the person is fully informed and competent to give consent and they have given consent of their own free will, and without coercion from others, Individuals have the right to withdraw consent at any time.

You should not seek consent to disclose personal information in circumstances where:

- someone has been hurt and information needs to be shared quickly to help them.
- obtaining consent would put someone at risk of increased harm.
- obtaining consent would prejudice a criminal investigation or prevent a person being questioned or caught for a crime they may have committed.
- the information must be disclosed regardless of whether consent is given, for example if a Court order or other legal obligation requires disclosure.

NB. The serious crimes indicated are those that may harm a child or adult; reporting confidential information about crimes such as theft or benefit fraud are not in this remit.

- Settings are not obliged to report suspected benefit fraud or tax evasion committed by adults associated with the setting, however, they are obliged to tell the truth if asked by an investigator.
- Parents who confide that they are working while claiming should be informed of this and should be encouraged to check their entitlements to benefits, as it may be beneficial to them to declare earnings and not put themselves at risk of prosecution.

Procedure for obtaining consent to store and share information

We gain consent to store and share information in the following ways:

- Application form – signed on application for a place. It confirms that the parent/carer has received and read the *07.01a families privacy notice* and gives consent for information being recorded and held
- Registration form – signed on registration. Confirms:
    - Permissions e.g consent to apply sun cream or share photos and regular local walks including forest trips
    - consent to share information about child with next provider/school/second setting, e.g regarding additional needs, or child development information.
    - that parent/carer has read the 09.01d Terms & conditions document
- Larger outing/excursion consent forms – signed for each outing to confirm attendance using Microsoft Forms.
- Notes on data collection is included as a footer on every form the parent signs.

Consent

- Parents share information about themselves and their families. They have a right to know that any information they share will be regarded as confidential as outlined in the *07.01a Families Privacy notice*. They should also be informed about the circumstances, and reasons for the setting being under obligation to share information.
- Parents are advised that their informed consent will be sought in most cases, as well as the circumstances when consent may not be sought, or their refusal to give consent overridden.
- Where there are concerns about whether to gain parental consent before sharing information, for example when making a Channel or Prevent referral the setting manager must seek the Data Protection Lead for clarification before speaking to parents.
- Consent must be informed – that is the person giving consent needs to understand why information will be shared, what will be shared, who will see

information, the purpose of sharing it and the implications for them of sharing that information.

Obtaining consent when parents are separated

- Consent to share need only be sought from one parent. Where parents are separated, this would normally be the parent with whom the child resides.
- Where there is a dispute, this needs to be considered carefully.
- Where the child is looked after, the local authority, as 'corporate parent' may also need to be consulted before information is shared.

Age for giving consent

- A child may have the capacity to understand why information is being shared and the implications. For most children under the age of eight years in a nursery or out of school childcare context, consent to share is sought from the parent, or from a person who has parental responsibility.
- Young persons (16-19 years) are capable of informed consent. Some children from age 13 onwards may have capacity to consent in some situations. Where they are deemed not to have capacity, then someone with parental responsibility must consent. If the child is capable and gives consent, this may override the parent's wish not to give consent.
- Adults at risk due to safeguarding concerns must be deemed capable of giving or withholding consent to share information about them. In this case 'mental capacity' is defined in terms of the Mental Capacity Act 2005 Code of Practice (Office of the Public Guardian 2007). It is rare that this will apply in the context of the setting.

Procedure for consent to share information

Consent to share information is gained by the following methods:

- Policies and procedures set out the responsibility of the setting regarding gaining consent to share information, and when it may not be sought or overridden.
- Information in leaflets to parents, or other leaflets about the provision, including privacy notices, term and conditions.
- Consent forms signed at registration (for example to apply sun cream/ photo permissions).
- Our data protection statement is included on every form the parent signs.
- Parent signatures on forms giving consent to share information about additional needs, or to pass on child development summaries to the next provider/school.

07.03 PROCEDURE: Client access to records

Under the General Data Protection Regulations there are additional rights granted to data subjects which must be protected by the setting.

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 the setting has compiled on them.

- If a parent wishes to see the file, a written request is made, which the setting acknowledges in writing, informing the parent that an arrangement will be made for him/her to see the file contents, subject to third party consent.

- Information must be provided within 30 days of receipt of request. If the request for information is not clear, the manager must receive legal guidance, for instance, from Law-Call for members of the Alliance. In some instances, it may be necessary to allow extra time in excess to the 30 days to respond to the request. An explanation must be given to the parent where this is the case. The maximum extension time is 2 months.
- A fee may be charged to the parent for additional requests for the same material, or any requests that will incur excessive administration costs.
- The setting manager informs the Data Protection lead and legal advice is sought.
- The parent may take a copy of the prepared file away, but it is never handed over without discussion.
- It is an offence to remove material that is controversial or to rewrite records to make them more acceptable. If recording procedures and guidelines have been followed, the material should reflect an accurate and non-judgemental account of the work done with the family.
- If a parent feels aggrieved about any entry in the file, or the resulting outcome, then the parent should be referred to section *10.2 Complaints procedure for parents and service users* of our *Working in Partnership with Parents* Policy.
- The law requires that information held must be accurate, and if a parent says the information held is inaccurate then the parent has a right to request 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, the setting retains the right not to change the entry but can record the parent's view. In most cases, a parent would have had the opportunity at the time to state their side of the matter, and this should have been recorded there and then.
- If there are any controversial aspects of the content of a client's file, legal advice must be sought. This might be where there is a court case between parents or where social care or the police may be considering legal action, or where a case has already completed and an appeal process is underway.
- A setting should never 'under-record' for fear of the parent seeing, nor should they make 'personal notes' elsewhere.

Procedure for preparing material for a subject access request

- The setting manager goes through the file with their line manager and ensures all documents are filed correctly, 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. The setting manager should always ensure that recording is of good quality, accurate, fair, balanced and proportionate. There should be a quality assurance processes in place to ensure that files are regularly checked and that any issues are addressed promptly.
- Each individual referred to as a third party is written to, explaining that the subject of the file has requested sight of the file which contains a reference to them, stating what this is. They are asked to reply in writing to the setting manager giving or refusing consent for disclosure of that material.
- Each family member noted on the file is a third party, so where there are separate entries pertaining to each parent, step-parent, grandparent etc, each of those have to be written to regarding third party consent.

- Members of staff should also be written to, but the setting reserves the right under the legislation to override a refusal for consent, or just delete the name and not the information.
- Copies of these letters and their replies are kept on the child's file.
- Agencies will normally refuse consent to share information, and the parent should be redirected to those agencies for a request to see their file held by that agency.
- Entries where you have contacted another agency may remain, for example, a request for permission from social care to leave in an entry where the parent was already party to that information.

07.04 PROCEDURE: Transfer of records

Records about a child's development and learning in the EYFS are made by the setting; to enable smooth transitions, appropriate information is shared with the receiving setting or school at transfer. Confidential records are passed on securely where there have been SEN or safeguarding concerns, as appropriate.

Transfer of development records for a child moving to another early years setting or school

- It is the managers' responsibility to ensure that records are transferred and closed, in accordance with the archiving procedures, set out below.
- If the Hampshire Safeguarding Children's Partnership (HSCP) retention requirements are different to the setting, the setting manager will liaise with their line manager, and seek legal advice if necessary.

Procedure for transfer of development and learning records

- The key person prepares a *9.13a Transition to school report*; summary of achievements in the prime and specific areas of learning and development in line with the procedure.
- The record contains a summary by the key person
- This record refers to any additional languages spoken by the child and their progress in all languages.
- The record also refers to any additional needs that have been identified or addressed by the setting and any action plans.
- It should be completed and shared with the parent prior to transfer. Parents are invited to a parents meeting to discuss the report.
- Records can be posted by registered delivery to a named person or delivered in person to the receiving school or setting.
- The parent will be given the opportunity to download a PDF copy or given a memory stick of the child's Tapestry Online Learning Journal before deletion.
- A record of transfer is kept

Transfer of confidential safeguarding, child protection, medical and SEN information

- Records will be shared confidentially of any special needs or disability and whether early help referrals, or child in need referrals or child protection referrals, were raised in respect of special educational needs or disability, whether there is an Action Plan (or other relevant plan, such as CIN or CP, or early help) and gives the name of the lead professional.
- The information shared with schools should also include whether the child is in receipt of, or eligible for EYPP or other additional funding.
- The receiving school/setting will need a record of child protection concerns raised in the setting and what was done about them. The responsibility for transfer of records lies with the originating setting, not on the receiving setting/school to make contact and request them.
- To safeguard children effectively, the receiving setting must be made aware of any current child protection concerns, preferably by telephone or at induction handover if arranged, prior to the transfer of written records. The child protection file must be

transferred to the receiving setting within 5 days for an in year transfer and 5 days after the start of a new term for an end of year transfer. A receipt of confirmation should be obtained.

- Parents should be reminded that sensitive information, about their child is passed onto receiving settings where there have been safeguarding concerns and should be asked to agree to this prior to the information being shared. Settings are obliged to share data linked to "child abuse" which is defined as physical injury (non-accidental) physical and emotional neglect, ill treatment and abuse. Parent/carers should be made aware what information will be passed onto another setting via *07.01a Families Privacy Notice.*
- Parents/carers should be asked to agree to this, however, where safeguarding concerns have reached the level of a referral being made to local children's social work services (either due to concerns that a child may be at risk of significant harm or that a child may be in need under Section 17 of the Children Act,) if consent is withheld the information will most likely need to be shared anyway. It is important that any decisions made to share or not share with or without consent are fully recorded.
- 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. It would be legitimate to share information without consent where: it is not possible to gain consent; it cannot be reasonably expected that a practitioner gains consent; and, if to gain consent would place a child at risk
- Copies of the last relevant initial child protection conference/review, as well as the last core group or child in need minutes can be given to the setting/school.
- For any safeguarding or welfare concerns that resulted in an early help referral being made, and if consent to share is withheld, legal advice is sought prior to sharing.
- The setting manager must review and update and archive any confidential information checking for accuracy, proportionality, and relevance, before this is copied and sent to the setting/school and ensure the remaining file is archived in line with the procedures set out below.
- If a parent wants to see the exact content of the safeguarding information to be transferred, they should go through the subject access request process. It is important that a child or other person is not put at risk through information being shared.
- If the level of a safeguarding concern has not been such that a referral was made for early help, or to children's social work services or police, the likelihood is that any concerns were at a very low level and if they did not meet the threshold for early help, they are unlikely to need to be shared as child abuse data with a receiving setting, however, the designated person should make decisions on a case by case basis, seeking legal advice is necessary.
- If a parent has objections or reservations about safeguarding information being transferred to the new setting, or if it is unclear what information should be included, the designated safeguarding lead will seek legal advice. Parents can request that any factual inaccuracies are amended prior to transfer.
- No other documentation from the child's personal file is passed to the receiving setting or school.

- Hampshire Safeguarding Childrens Partnership require settings to hand on all information on safeguarding and child protection concerns and not keep a copy of this.

Procedure for transfer of confidential safeguarding, child protection, medical and SEN information

- The setting manager establishes a named person at the receiving school to transfer any confidential records to.
- *07.04c Transfer of safeguarding records form* or *07.04d Transfer of SEN or medical records* will be completed.
- The designated safeguarding lead should check the quality of information, prior to transfer. They should ensure that any information to be shared is accurate, relevant, balanced and proportionate.
- If no referrals have been made for early help or to children's social work services and police, there should not be any significant information being shared with the receiving school or setting, which is unknown to a parent.
- In the event that HSCP requirements are different to the setting's this must be explained to the parent, and a record of the discussion should be signed by parents to indicate that they understand how the information will be shared, in what circumstances, and who by.
- Prior to sharing the information with the receiving setting the designated safeguarding lead should check HSCP retention procedures and if it becomes apparent that the HSCP procedures are materially different to setting's procedures this is brought to the attention of the designated person's line manager, who will agree how to proceed.
- If a child protection plan or child in need plan is in place *06.1a Child welfare and protection summary* is also photocopied and a copy is given to the receiving setting or school, along with the date of the last professional meeting or case conference.
- If a S47 investigation has been undertaken by the local authority a copy of the child welfare and protection concern summary form is given to the receiving setting/school.
- Where an early help assessment has been raised in respect of welfare concerns, the name and contact details of the lead professional are passed on to the receiving setting or school**.**
- If the setting has a copy of a current plan in place due to early help services being accessed, a copy of this should be given to the receiving setting, with parental consent.
- Where there has been a S47 investigation regarding a child protection concern, the name and contact details of the child's social worker will be passed on to the receiving setting/school, regardless of the outcome of the investigation.
- Where a child has been previously or is currently subject to a child protection plan, or a child in need plan, the name and contact details of the child's social worker will be passed onto the receiving setting/school, along with the dates that the relevant plan was in place for.
- This information is posted (by 'signed for' delivery) or taken to the school/setting, addressed to the setting's or school's designated person for child protection and marked confidential.
- Electronic records must only be transferred by a secure electronic transfer mechanism to a named individual responsible for safeguarding. An email requesting

email confirmation of receipt of electronically sent information and store digitally on child's digital file in line with retention schedule.

- Copies of the last relevant initial child protection conference/review, as well as the last core group or child in need minutes can be given to the setting/school.
- The setting manager must review and *update 06.1a Child welfare and protection summary,* checking for accuracy, proportionality, and relevance, before this is copied and sent to the setting/school.
- The setting manager ensures the remaining file is archived in line with the procedures set out below.
- No other documentation from the child's personal file is passed to the receiving setting or school. The setting keeps a copy of any records in line with required retention periods.
  All information on safeguarding and child protection concerns as passed onto the next setting. Do not keep a copy. In line with HCC requirements.

Procedure for archiving records and children's files

Use the retention schedule *(07.04a LF Retention Schedule)* to inform when how to archive information safely and securely.

- Paper documents are removed from the child's file and placed in a robust folder, labelled with the date, as per the retention schedule.
- This is sealed and stored in a safe place i.e. a locked cabinet for three years or until the next Ofsted inspection conducted after the child has left the setting, and can then be destroyed in line with the retention policy
- For web-based or digital children's files, the setting manager / business administrator must also use the archiving procedure, and records details of what needs to be retained/destroyed. The designated person must make arrangements to ensure that electronic files are deleted/retained as required in accordance with the required retention periods in the same way as paper-based files.
- Health and safety records and some accident records pertaining to a child are stored for longer. Again, this is in line with required retention periods.
- The designated person writes clearly on the front of the envelope the length of time the file should be kept before destruction.
- From January 2023, Little Fishes has maintained a database of records which have been archived. This is *07.04b LF Archive, Transfer or Destruction Record*.

Procedure for destruction of records

Use the retention schedule *(07.04a LF Retention Schedule)* to inform when how to destroy information safely and securely.

Where records have been identified for destruction, they should be disposed of in an appropriate way. All paper records containing personal information, or sensitive policy information should be shredded before disposal, where possible. All electronic information will be deleted.

All information must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances.

From January 2023, Little Fishes maintains a database of records which have been destroyed; *07.04b LF Archive, Transfer or Destruction Record 2023.* The date of destruction, File title/description, Number of files and method of destruction are recorded.

Legal references

- General Data Protection Regulation 2018
- Freedom of Information Act 2000
- Human Rights Act 1998
- Statutory Framework for the Early Years Foundation Stage (DfE 2023)
- Data Protection Act 2018

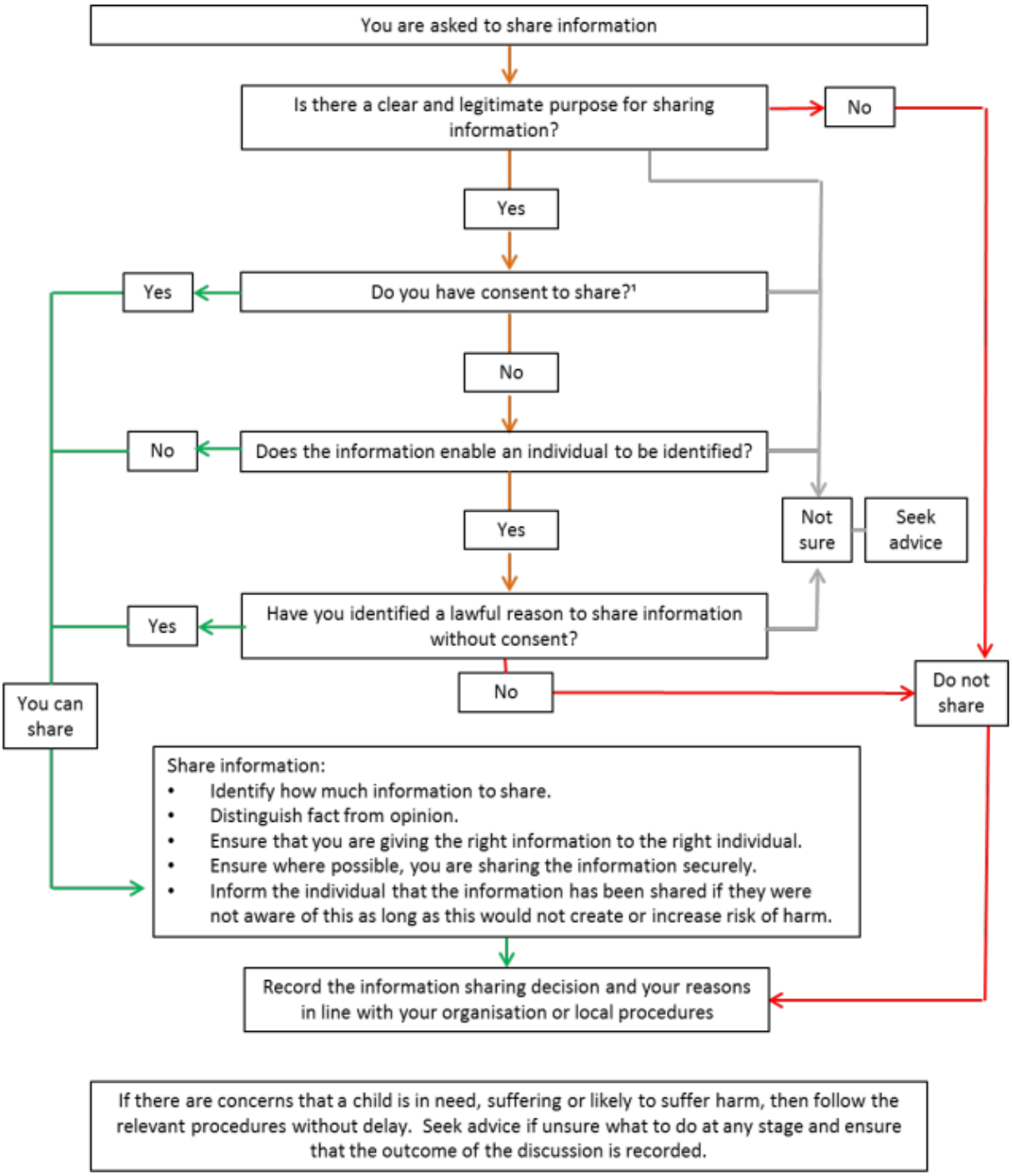
Further guidance

- Working Together to Safeguard Children (DfE 2023), www.gov.uk/government/publications/working-together-to-safeguard-children--2
- Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers. (HMG 2024) The seven golden rules for sharing information will be especially useful Information_sharing_advice_practitioners_safeguarding_services
- Keeping children safe in education 2024: part one
- What to do if you're Worried a Child is Being Abused (HMG 2015) www.gov.uk/government/publications/what-to-do-if-youre-worried-a-child-is-being-abused--2
- Mental Capacity Act 2005 Code of Practice (Office of the Public Guardian 2007) www.gov.uk/government/publications/mental-capacity-act-code-of-practice
- The Information Commissioner's Office which includes information about your obligations and how to comply, including protecting personal information www.ico.gov.uk/ or helpline 0303 123 1113.
- https://www.gov.uk/guidance/data-protection-in-schools - Guidance to support schools with data protection activity, including compliance with the UK GDPR.

APPENDIX 1: Location of children's personal records

- Children's personal files contain:
  - Developmental and learning records
  - SEND support requirements and plans
  - Reports by outside agencies
  - Additional focussed intervention provided by the setting e.g. support for behaviour, language or development that needs an Action Plan at setting level
  - Records of any meetings held
  - Health care plans
  - Archived medication forms and allergy risk assessments
- The welfare file contains:
  - Low level observations regarding welfare
  - Records of notable conversations with parents
  - Background information forms
  - Safeguarding record of concerns that were judged as low level
- The registration folder contains:
  - Personal details,
  - Application and registration form
    Consent forms.
- The register contains:
  - Permissions Form: parental permission for photos, outings, nappy cream, sun cream and second setting information
  - Allergy and medical information
    - Medical summary form for all adults and children in setting
    - Current Health care plans
    - summary for child
    - Current allergy risk assessments
    - Current Medication consent forms
  - Daily attendance records for children
  - Emergency contact details (children and staff)
  - Attendance data tracking and book recording reasons for absence
- The emergency/outings bag contains:
  - Emergency contact details (children and staff)
  - Copies of child health care plans
  - Copies of allergy risk assessments and medication consent forms
- The safeguarding file contains:
  - Safeguarding concerns
  - Correspondence and reports
  - All letters and emails to and from other agencies
  - Confidential reports from other agencies
- Financial records and information (such as copies of contract, days and times, record of fees, any fee reminders or records of disputes about fees are kept as paper files in a filing cabinet which is always locked when not in use, or digitally on a secure internet-based cloud storage platform which has restricted access.

APPENDIX 2: Flowchart of when and how to share information



1. Consent must be unambiguous, freely given and may be withdrawn at any time

This policy was adopted on: 31/01/2023
Reviewed: February 2024
Next review date: February 2025
Name of Manager: Amber Delves
Signature: A. Delves