07 Record keeping policy

Alongside associated procedures, this policy was adopted by *Esklet's Pre School* September 2026

Aim

We have record keeping systems in place for the safe and efficient management of the provision and to meet the needs of the children; that meet legal requirements for the storing and sharing of information within the framework of the GDPR and the Human Rights Act.

Objectives

- Children's records are kept in personal files, divided into appropriate sections, and stored separately from their developmental records, or are kept electronically on management software systems.
- Children's personal files contain registration information as specified in procedure 07.1 Children's records and data protection.
- Children's personal files contain other material described as confidential as required, such as Early Help Assessments, Early Support information or Education, Health and Care Plan (EHCP), case notes including recording of concerns, discussions with parents/carers, and action taken, copies of correspondence and reports from other agencies.
- Ethnicity data is only recorded where parents/carers 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 have a right or professional need to see them. Client access to records is provided for within procedure 07.3 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.
- Staff know how to share information if they believe a child is in need or at risk of suffering harm.
- Staff record when and to whom information has been shared, why information was shared and parental consent will be sought where appropriate; however, consent is not required where there is a safeguarding concern, a statutory duty to share information, or another lawful basis for disclosure.
- Where consent has not been given and staff have taken the decision, in line with Information Sharing Duty, 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.

Records

The following information and documentation are also held:

- 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
- Information about staff qualifications, identity checks and references that have been completed during the recruitment process
- a daily record of all children looked after on the premises, their hours of attendance and their named key person
- certificate of registration displayed and shown to parents/carers on request
- records of risk assessments
- record of complaints and their resolutions
- record of accidents or injuries and first aid treatment. to include steps that were taken and if incidents were reported to Health and Safety Executive (HSE) and/or Ofsted.
- record of any safeguarding allegations against a member of staff, visitors or volunteers

Legal references

General Data Protection Regulation 2018

Freedom of Information Act 2000

Human Rights Act 1998

Statutory Framework for the Early Years Foundation Stage

Data Protection Act 2018

Further guidance

Information Sharing Duty
Business management mini-guide (Alliance publication)

07.1 Children's records and data protection

All information is kept in line with the Esklet's Pre School Privacy Notice. This is shared with parents and carers when a child or young person is registered for a service.

Parents/carers are asked to sign informed consent to record and sharing information prior to their child/young person attending a 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 unless there is a lawful basis to do so.

The setting is committed to protecting personal information and ensuring that all data is collected, stored, used and shared in accordance with UK data protection legislation. Personal information will only be accessed by those who need it and will be handled securely, confidentially and appropriately.

The setting recognises that data protection legislation does not prevent the sharing of information where there is a lawful basis to do so. In line with safeguarding responsibilities and the statutory Information Sharing Duty, relevant information may be shared with appropriate professionals and agencies when it is necessary to safeguard a child, promote their welfare, assess needs, identify risks or provide support.

Wherever possible, the setting will be transparent with children, parents and carers about how information is used and shared. Consent will be obtained where required; however, consent is not always necessary when there are safeguarding concerns or another lawful basis for sharing information. Staff must not allow concerns about data protection to delay or prevent appropriate action being taken to protect a child.

All information-sharing decisions will be necessary, proportionate, relevant, accurate, timely and recorded appropriately. Information will only be shared with those who have a legitimate need to know and will be transferred securely in accordance with local safeguarding procedures and statutory guidance.

Principles of data protection: lawful processing of data

Personal data shall be:

a) *processed lawfully, fairly and in a transparent manner in relation to the data subject*

b) *collected for specified, explicit and legitimate purposes and not further processed in a manner that is not compatible for these purposes*

c) *adequate, relevant and necessary in relation to the purposes for which they are processed*

d) *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*

e) *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*

f) *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)

Educators should process data, record and share information in line with the principles above.

During an outbreak of serious illness of disease there may be the need to keep additional records as part of outbreak management. A record is kept of individual cases of children/families who are self-isolating due to symptoms as per usual record-keeping procedures. In all cases the principles of data protection are maintained at [name of setting]

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, Ofsted inspector, childminder agency, by the successors of the educators 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 factual, 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 at Esklet's Pre School

- 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 07.1a Privacy notice and should 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, unless there is a lawful basis to do so.
- 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 there is a lawful basis to do so, and 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. Educators are aware of information sharing processes in line with Information Sharing Duty 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.

Children's personal files at Esklet's Pre School (where nursery management software is not used)

- For paper records, appropriate files should be used. These are made of robust card (not ring binders) and have plastic or metal binders to secure documents. File dividers must be inserted into each file.
- The sections contained are as follows:
  - personal details: registration form and consent forms – additional emergency contact numbers should be provided
  - contractual matters: copies of contract, days and times, record of fees, any fee reminders or records of disputes about fees.
  - SEND support requirements
  - 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
  - welfare and safeguarding concerns, correspondence and reports, all letters and emails to and from other agencies and confidential reports from other agencies
- Children's personal files are kept in a filing cabinet, which is always locked when not in use.
- Correspondence in relation to a child is read, any actions noted, and filed immediately
- Access to children's personal files 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 other staff as authorised by the setting manager.
- 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 if authorisation is seen.

provide early education and childcare services and to fulfil the contractual arrangement you have entered. This includes using your data in the following ways:

- To support your child's wellbeing and development.
- To effectively manage any special education, health or medical needs of your child whilst at the setting.
- To carry out regular assessment of your child's progress and to identify any areas of concern.
- To maintain relevant contact about your child's wellbeing and development.
- To contact you in the case of an emergency.
- To process your claim for funded early education and childcare , if applicable.
- To enable us to respond to any questions you ask.
- To keep you updated about information which forms part of your contract with us.
- To notify you of service changes or issues.
- To send you our e-newsletter, if you have subscribed to it.

With your consent, we would also like to:

- Collect your child's ethnicity and religion data for monitoring purposes.
- Record your child's activities for their individual learning journal (this will often include photographs and videos of children during play).
- Sign you up for our free parent e-newsletter which provides resources and useful information for parents.
- Transfer your child's records to the receiving school when s/he transfers.

If we wish to use any images of your child for training, publicity or marketing purposes we will seek your written consent for each image we wish to use. You are able to withdraw your consent at any time, for images being taken of your child and/or for the transfer of records to the receiving school, by confirming so in writing to the setting. You can also unsubscribe from receiving our parent e-newsletter by notifying the setting.

We have a legal obligation to process safeguarding related data about your child should we have concerns about her/his welfare.

Who we share your data with

As a registered early years provider to deliver early education and childcare services it is necessary for us to share data about you and/or your child with the following categories of recipients:

- Ofsted, or the childminder agency (if registered with an agency) when there has been a complaint about the early education and childcare service or during an inspection.

- Banking services to process chip and pin and/or direct debit payments.
- The local authority if you claim up to 30 hours funded early education and childcare.
- The governments eligibility checker as above, if applicable.
- Our insurance underwriter, where applicable.
- An email newsletter service, where you have given consent to receive our e-newsletter.

We will also share your data:

- If we are legally required to do so, for example, by a law enforcement agency, or court.
- To enforce or apply the terms and conditions of your contract with us.
- To protect your child and other children; for example, by sharing information with medical services, social services, or the police.
- If it is necessary to protect our rights, property, or safety or to protect the rights, property, or safety of others.
- With the school that your child will be attending, when they transfer, if applicable.
- If we transfer the management of the provision out or take over any other organisation or part of it, in which case we may disclose your personal data to the prospective seller or buyer so that they may continue using it in the same way.

Our nursery management and communication software provider may be able to access your personal data when carrying out maintenance task and software updates on our behalf. However, we have a written agreement in place which place this company under a duty of confidentiality.

We will never share your data with any organisation to use for their own purposes.

How do we protect your data?

We take the security of your personal data seriously. We have internal policies and strict controls in place to try to ensure that your data is not lost, accidentally destroyed, misused, or disclosed and to prevent unauthorised access.

Where we engage third parties to process personal data on our behalf, they are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Where do we store your data?

All data you provide to us is stored on secure computers or servers located within the UK or European Economic Area. We may also store paper records in locked filing cabinets.

Our third-party data processors will also store your data on secure servers which may be situated inside or outside the European Economic Area. They may also store data in paper files.

How long do we retain your data?

We retain your data in line with our retention policy a summary is below:

- You and your child's data, including registers are retained 3 years after your child no longer uses the setting, or until our next Ofsted, or childminder agency inspection after your child leaves our setting.
- Medication records and accident records are kept for longer according to legal requirements.
- Learning journeys are maintained by the setting and available at your request when your child leaves. Records are kept and archived in line with our data retention policy.
- In some cases (child protection or other support service referrals), we may need to keep your data longer, only if it is necessary to comply with legal requirements. We will only keep your data for as long as is necessary to fulfil the purposes it was collected for and in line with data protection laws.

Your rights with respect to your data

As a data subject, you have several rights. You can:

- request to access, amend or correct the personal data we hold about you and/or your child
- request that we delete or stop processing your and/or your child's personal data, for example where the data is no longer necessary for the purposes of processing or where you wish to withdraw consent
- request that we transfer your and your child's personal data to another person

If you wish to exercise any of these rights at any time please contact the manager at the setting by email, telephone or when you attend the setting.

How to ask questions about this notice

If you have any questions, comments, or concerns about any aspect of this notice or how we handle your data please contact the manager at the setting.

How to contact the Information Commissioner Office (ICO)

If the manager is not able to address your concern, please contact *[Insert details of setting manager's line manager/owner/director/trustee]*

If you are concerned about the way your data is handled and remain dissatisfied after raising your concern, you have the right to complain to the Information Commissioner Office (ICO). The ICO can be contacted at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF or https://ico.org.uk/.

Changes to this notice

We keep this notice under regular review. Any changes to this notice will be shared with you so that you may be aware of how we always use your data.

07.2 Confidentiality, recording and sharing information

Most things that happen between the family, the child and the setting are confidential to Esklet's Pre School. Confidentiality will be respected wherever possible. However, where information may be relevant to safeguarding a child or promoting their welfare, information may be shared with appropriate agencies in accordance with statutory guidance, safeguarding legislation and data protection requirements, 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. Normally parents/carers should give informed consent before information is shared, but in some instances, such as if this may place a child at risk, or a serious offence may have been committed, parental consent should not be sought before information is shared. Local Safeguarding Partnership (LSP) 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/carers or anyone else outside of the organisation, unless in a formal and lawful way.
- 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.
- It is important that members of staff explain to parents/carers that sometimes it is necessary to write things down in their child's file and explain the reasons why.
- When recording general information, staff should ensure that records are dated correctly, and the time is included where necessary and signed.
- Welfare/child protection concerns are recorded on 6.1b Safeguarding incident reporting form. Information is clear and unambiguous (fact, not opinion), although it may include the educator'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 action taken to deal with the concern. The appropriate recording format is filed within the child's file.
- Information shared with other agencies is done in line with these procedures and Information Sharing Duty.

- Where a decision is made to share information (or not), reasons are recorded.
- Staff may use a computer to type reports, or letters. Where this is the case, the typed document is deleted from the computer and only the hard copy is kept.
- Electronic copy is downloaded onto a disc, labelled with the child's name and stored in the child's file. No documents are kept on a hard drive because computers do not have facilities for confidential user folders.
- The setting is registered with the Information Commissioner's Office (ICO). Staff are expected to follow guidelines issued by the ICO, at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/
- 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, 2026); Information Sharing Duty, 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)

Confidentiality definition

- 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.
- 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/carers regard this information as confidential or not.
- Parents/carers sometimes share information about themselves with other parents/carers as well as staff; the setting cannot be held responsible if information is shared beyond those parents/carers whom the person has confided in.
- Information shared between parents/carers 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.
- Educators 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.

Breach of confidentiality

- 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.
- Procedure 07.1 Children's records and data protection must be followed.

Exception

- GDPR enables information to be shared lawfully within a legal framework. The Data Protection Act 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 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 educators to share without consent if there is a lawful basis to do so, if consent cannot reasonably be gained, or if gaining consent would place a child at risk.
-
- Confidential information may be shared without consent and where a child may be at risk of harm or where information is required to safeguard or promote a child's welfare. In accordance with the statutory Information Sharing Duty, the setting has a responsibility to share relevant information with appropriate professionals and agencies when it may assist in assessing need, identifying risk, making decisions or providing support for a child and their family.
- The Data Protection Act 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 designated person who can provide support, and sometimes ensure protection, through appropriate structures and procedures.

Obtaining consent

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 clients, however, they are obliged to tell the truth if asked by an investigator.
- Parents/carers who confide that they are working while claiming should be informed of this and should be encouraged to check their entitlements to benefits, as they it may be beneficial to them to declare earnings and not put themselves at risk of prosecution.

Consent

- Parents/carers 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 07.1a Privacy notice. They should also be informed about the circumstances, and reasons for the setting being under obligation to share information in line with the Information Sharing Duty.
- Parents/carers 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 inform their line manager for clarification before speaking to parents/carers.

- 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.

Separated parents/carers

- Consent to share need only be sought from one parent/carer. Where parents/carers are separated, this would normally be the parent/carer 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/carer, 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/carer'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.

Ways in which consent to share information can occur

- 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/carers, or other leaflets about the provision, including privacy notices.
- Consent forms signed at registration (for example, to apply sun cream).
- Notes on confidentiality included on every form the parent/carer signs.
- Parent/carer signatures on forms giving consent to share information about additional needs, or to pass on child development summaries to the next provider/school.

Further guidance

Working Together to Safeguard Children

Information Sharing Duty

07.3 Client access to records

Under the General Data Protection Regulations there are additional rights granted to data subjects which must be protected by Esklet's Pre School

The parent/carer 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/carer wishes to see the file, a written request is made, which the setting acknowledges in writing, informing the parent/carer 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/carer where this is the case. The maximum extension time is 2 months.
- A fee may be charged to the parent/carer for additional requests for the same material, or any requests that will incur excessive administration costs.
- The setting manager informs their line manager/owner/committee and legal advice is sought.
- The setting manager goes through the file 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 and should have quality assurance processes in place to ensure that files are checked for quality regularly and that any issues are addressed promptly.
- Each of those individuals are 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.
- 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/carer 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/carer was already party to that information.

- Each family member and/or carer noted on the file is a third party, so where there are separate entries pertaining to each parent/carer, stepparent, grandparent, etc., each of those must 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.
    - 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, then the refusal may be granted.
    - If that information is the basis of a police investigation, then refusal should also be granted.
    - If the information is not sensitive, then it is not in the setting's interest to withhold that information from a parent. It is a requirement of the job that if a member of staff has a concern about a child and this is recorded the parents/carers are told this at the start and in most cases, concerns that have been recorded will have been discussed already, so there should be no surprises.
    - The member of staff's name can be removed from an entry, but the parent/carer may recognise the writing or otherwise identify who had provided that information. In the interest of openness and transparency, the setting manager may consider overriding the refusal for consent.
    - In each case this should be discussed with members of staff and decisions recorded.
- When the consent/refusals have been received, the setting manager takes a photocopy of the whole file. On the copy file the document not to be disclosed is removed (e.g., a case conference report) or notes pertaining to that individual in the contact pages blanked out using a thick marker pen.
- The copy file is then checked, and legal advisors verify that the file has been prepared appropriately, for instance, in certain circumstances redaction may be appropriate, for instance if a child may be damaged by their data being seen by their parent/carer, e.g., if they have disclosed abuse. This must be clarified with the legal adviser.
- The 'cleaned' copy is then photocopied again and collated for the parent/carer to see.
- The setting manager informs the parent/carer that the file is now ready and invites him/her to make an appointment to view it.
- The setting manager and their line manager/trustee/committee member, etc., meet with the parent/carer to go through the file, explaining the process as well as what the content records about the child and the work that has been done. Only the persons with parental responsibility can attend that meeting, or the parent's/carer's legal representative or interpreter.
- The parent/carer may take a copy of the prepared file, 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/carer feels aggrieved about any entry in the file, or the resulting outcome, then the parent/carer should be referred to section 10.2 Complaints procedure for parents/carers and service users.
- The law requires that information held must be accurate, and if a parent/carer says the information held is inaccurate then the parent/carer 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/carer, the setting retains the right not to change the entry but can record the parent's/carer's view. In most cases, a parent/carer 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/carer seeing, nor should they make 'personal notes' elsewhere.

Further guidance

The Information Commissioner's Office https://ico.org.uk/ or helpline 0303 123 1113.

07.4 Transfer of records

Records about a child's development and learning in the EYFS are made by the staff at Esklet's Pre School 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 concerns, as appropriate.

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

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

Development and learning records

- The key person prepares a summary of achievements in the prime and specific areas of learning and development
- 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.
- The record also refers to any special needs or disability and whether early help referrals, or child in need (CIN) referrals or child protection (CP) 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 summary shared with schools should also include whether the child is in receipt of, or eligible for EYPP (Early Years Pupil Premium) or other additional funding.
- The record contains a summary by the key person and a summary of the parent/carers' view of the child.
- The document may be accompanied by other evidence such as photos or drawings that the child has made.
- The setting will use the local authority's assessment summary format or transition record, where these where provided.
- Whichever format of assessment summary is used; it should be completed and shared with the parent/carer prior to transfer.

Transfer of confidential safeguarding and child protection information

- 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, prior to the transfer of written records.
- Parents/carers 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.
- 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.
- 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.
- 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 safeguarding lead should make decisions on a case by case basis, seeking legal advice as necessary.

- The designated safeguarding lead person should check the quality of information to be transferred prior to transfer, ensuring that any information to be shared is accurate, relevant, balanced and proportionate. Parents/carers can request that any factual inaccuracies are amended prior to transfer.
- If a parent/carer 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 no referrals have been made for early help or to children's social work services and police, there should not normally be any significant information which is unknown to a parent/carer being shared with the receiving school or setting.
- If a parent/carer 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 person will seek legal advice.
- If LSP requirements are different to the setting's this must be explained to the parent/carer, and a record of the discussion should be signed by parents/carers 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 LSP retention procedures and if it becomes apparent that the LSP procedures are materially different to setting's procedures this is brought to the attention of the designated safeguarding lead'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 settings or schools designated person for child protection and marked confidential. Electronic records

must only be transferred by a secure electronic transfer mechanism, or after the information has been encrypted.

- Parent/carers should be made aware what information will be passed onto another setting via 07.1a Privacy notice.
- 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 safeguarding records in line with required retention periods.

Archiving children's files

- Paper documents are removed from the child's file, taken out of plastic pockets, and placed in a robust envelope, with the child's name and date of birth on the front and the date they left.
- The setting manager writes clearly on the front of the envelope the length of time the file should be kept before destruction.

  This is sealed and placed in an archive box and stored in a safe place i.e. a locked cabinet for three years or until the next Ofsted or childminder agency inspection conducted after the child has left the setting and can then be destroyed.
- For web-based or electronic children's files, the designated person must also use the archiving procedure, and records details of what needs to be retained/destroyed. The designated person must plan 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 in line with required retention periods.