7.1 DATA PROTECTION & RECORD KEEPING POLICY

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. They meet the legal requirements for the storing and sharing of information within the framework of the GDPR and the Human Rights Act.

We adhere to the Cheam Baptist Church Data Protection Policy along with our own Data Protection & Record Keeping Policy.

Objectives

- Children's records are kept in named personal files, divided into appropriate sections, and stored separately from their developmental records (learning journeys) or are kept electronically on the Pre-school One-drive.
- Children's personal files contain registration information as specified in the Pre-school policy 7.2 Children's records and data protection.
- Children's personal files contain other material described as confidential as required, such as 2-year checks, Early Support information or Education, Health and Care Plan (EHCP), case notes including recording of concerns, discussions with parents/carers, and any 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 need to know. Client access to records is provided for within procedure 07.4 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 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. 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
- 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 on request

- records of risk assessments
- record of complaints

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 2025)

Data Protection Act 2018

Further guidance

Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers (HMG 2018)

7.2 RECORD KEEPING PROCEDURES – CHILDREN'S RECORDS AND DATA PROTECTION

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 is 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.

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, 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 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. (Body map should be used if possible).

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 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.
- 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 an educator is unable to gain consent, cannot 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. Educators 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.

Children's personal files

Some of these will be kept as paper records and some as digital records.

- Categories of information are as follows:
  - personal details: registration form and consent forms.
  - 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.
- Children's personal files are not handed over to anyone else to look at.
- Children's files may be handed to Ofsted or Local Authority Advisors as part of an inspection or investigation.

7.3 RECORD KEEPING PROCEDURES – CONFIDENTIALITY, RECORDING AND SHARING INFORMATION

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. 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 Children Partners (LSCP) 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 DSLs 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 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 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.
- 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.

- The setting, through Cheam Baptist Church, 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/guidance-index/
- 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)

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.
- Staff ensure that parents/carers understand that information given confidentially will be shared appropriately within the setting (for instance with a DSL, Manager) and should not agree to withhold information from the DSL or 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.

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 educators 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 DSL 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 the Pre-school's Privacy notice. They should also be informed about the circumstances, and reasons for the setting being under obligation to share information.
- 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 Manager/DSL must seek advice 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.

Ways in which consent to share information can occur

- Policies and procedures set out the responsibility of the Pre-school 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.
- Notes on confidentiality included on forms 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 (DfE 2025)

Information Sharing: Advice for Practitioners Providing Safeguarding Services to Children, Young People, Parents and Carers (HMG 2024)

What to do if you're Worried a Child is Being Abused (HMG 2015)

Mental Capacity Act 2005 Code of Practice (Office of the Public Guardian 2007)

7.4 RECORD KEEPING PROCEDURES – CLIENT ACCESS TO FILES

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

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.
- 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 Manager informs the Pre-school Committee and legal advice is sought if necessary.
- The 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 Manager should always ensure that recording is of good quality, accurate, fair, balanced and proportionate.
- Each of third party 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 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 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.
- 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 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 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 (if necessary) 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 Manager informs the parent/carer that the file is now ready and invites him/her to make an appointment to view it.
- The Manager and their line manager/trustee/committee member etc… (if required) 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.
- 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.

7.5 RECORD KEEPING PROCEDURES – TRANSFER OF RECORD

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 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.

Development and learning records

- The key person prepares a Transition Report which is a summary of achievements in the prime areas of learning and development.
- The Transition Report refers to:
    - Any additional languages spoken by the child.
    - Any additional needs that have been identified or addressed by the setting and any action plans.
    - 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.
    - Whether the child is in receipt of, or eligible for EYPP or other additional funding.
    - A summary by the key person and a summary of the parent/carers' view of the child.
- The setting will use the local authority's assessment summary format or transition record, where these where provided.
- The Transition Report is 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. It is the responsibility of the Pre-school to send these.
- 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.

- 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 DSL should make decisions on a case by case basis, seeking legal advice is necessary.
- The DSL 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 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 DSL will seek legal advice.
- Any Child Protection & Safeguarding information, including concerns, referrals, assessments, plans, meetings, contact details of professionals involved, dates, investigations are photocopied and a copy is given to the receiving setting or school.
- 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, 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.
- The setting manager ensures the remaining file is archived in line with the procedures set out below. 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 and stored in the Storage Filing Cabinets upstairs for three years or until the next Ofsted inspection conducted after the child has left the setting and can then be destroyed.
- The Manager 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.

Reviewed March 2026
To be reviewed March 2027