7.0 DATA PROTECTION AND INFORMATION SHARING POLICY

September 2022

LAST UPDATED: DECEMBER 2023

Lloyd Park Children's Charity

Charity number 1102134

Contents

Data Protection and Information Sharing Policy 2
Objectives 3
Principles of data protection: lawful processing of data 4
General safeguarding recording principles 5
Storing Families Data 6
Confidentiality, Recording and Sharing Information 7
Breach of confidentiality 9
Data Protection Breach Procedure 9
Consent 10
Access to Records 13
Transfer of records 15
Transfer of confidential safeguarding and child protection information 16
Archiving files 19
Legal references 19
Further guidance 19

Data Protection and Information Sharing Policy

Introduction

At The Lloyd Park Children's Charity safety is at the heart of everything we do. Ensuring that we safely and securely hold your information to fulfil our legal obligations and that we do this with care and consideration for our users and employees is our utmost concern.

'Sharing information is an intrinsic part of any frontline practitioners' job when working with children and young people. The decisions about how much information to share, with whom and when, can have a profound impact on individuals' lives. It could ensure that an individual receives the right services at the right time and prevent a need from becoming more acute and difficult to meet. At the other end of the spectrum it could be the difference between life and death.'

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

We are registered with the Information Commissioner's Office (ICO), Reference Number: Z8669908. Staff are expected to follow guidelines issued by the ICO, at https://ico.org.uk/for-organisations/guidance-index/

Record Keeping

We have record keeping systems in place for the safe and efficient management of data 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

Across The Lloyd Park Children's Charity:

- Records are kept on our protected network and/or secure databases. Hard copies are stored in locked cupboards.
- 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.
- Ethnicity data is only recorded where parents have identified the ethnicity of their child themselves.
- 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.

Within the Day Care setting:

- Records are kept in personal files and stored separately from their developmental records and contain registration information as specified in section titled 'Family's records and data protection'
- Personal files contain other material described as confidential as required, such as Common Assessment Framework assessments, Early Support information or Education, Health and Care Plan (EHCP, case notes including recording of concerns, discussions with parents, and action taken, copies of correspondence and reports from other agencies.

- Confidentiality is maintained by secure storage of files in a locked cabinet with access restricted to those who need to know. Access to records information can be seen in section titled 'Access to Records'.

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 contact with children
- a daily record of all children looked after on the premises, their hours of attendance.
- certificate of registration displayed and shown to parents on request
- records of risk assessments
- record of complaints

Family's records and data protection

During an outbreak of serious illness of disease (such as Covid-19) 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.

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)

g) *Accountability*

Practitioners 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.
- 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.

The principles of GDPR and effective safeguarding recording practice are upheld: K

- 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. 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.
- 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.
- If a child attends more than one setting, a two-way flow of information is established between the parents/carers, and other providers.

Storing Families Data

- Appropriate files must be used. This includes electronic and hard copies. All data you provide to us is stored on secure computers or servers, with only authorised users having access. We use Microsoft 365 Software.
- The sections contained are as follows:
  - personal details: registration form and consent forms.
  - contractual matters (Care end Education Only): 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/ family personal files are kept in a filing cabinet, which is always locked when not in use.
- Correspondence in relation to a child/family 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 manager, deputy or designated person for child protection, the child's key person, or other staff as authorised by the 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 as long as authorisation is seen.
- Children and Family Centre records are stored securely on the mandatory database provided by LBWF. This is accessed by our local partners from The London Borough of Waltham Forest (LBWF), HENRY, NELFT and Tower Hamlets GP Care Group and is controlled by LBWF.

Confidentiality, Recording and Sharing Information

Most things that happen between the family, the child and the setting are confidential to The Lloyd Park Children's Charity. 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. Normally parents 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 Partners (LSP) procedures should be followed when making referrals, and advice sought if there is a lack of clarity about whether or not 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.
- 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 initially recorded on CP1 forms. 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 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 and these are saved securely on our protected network.

For Guidance for Staff please refer to our Safeguarding Policy.

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, unless found to be a risk to the child.
- Parents sometimes share information about themselves with other parents as well as staff; TLPCC 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 TLPCC 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 TLPCC.
- 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.

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.

Data Protection Breach Procedure

All personal data breaches must be reported immediately to the Chief Executive Officer, who will assign an appointed person within the organisation to lead (normally the Data Protection Lead). The appointed person will then follow the following steps:

1. Establish the facts and assess the damage.

Record details such as when the data breach occurred, how many data records are affected, what likely risk to individuals there is as a result of the breach.

2. Take immediate technical action.

Disconnect devices, ensure logging is still enabled and change passwords.

3. Communicate internally and prepare external communications.

Contact key stakeholders in the company/organisation and set up a project team to manage the data breach project. Start working on communication and PR plans asap.

4. Audit the data breach

Identify the systems compromised and the data exposed. Identify the cause of the breach.

5. Report to the ICO, if meets the breach criteria, within 72 hours of becoming aware of it, even if we do not have all the details yet.

6. Document all breaches even if we do not need to report them.

After the data protection breach is over, appropriate team members will meet and reflect on it and look at the impact on stakeholders. We will look at how such a data breach can be avoided in the future. We will assess the damage done to our Charity.

Consent

Exceptions

- 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.
- 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 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 (see section titled 'Exceptions'). 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.

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 our '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 or not 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
- 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

- 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.

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.
- Through privacy notices.
- Consent forms signed at registration (for example to apply sun cream).
- Parents sign LBWF Children and family Centre Registration Form at registration to confirm that they understand the data protection GDPR statement provided.
- Parent signatures on forms giving consent to share information about additional needs, or to pass on child development summaries to the next provider/school.

Access to Records

Under the General Data Protection Regulations there are additional rights granted to data subjects which must be protected by The Lloyd Park Children's Charity.

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 manager informs their line manager and legal advice is sought.
- The 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 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 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 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.
    - 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 TLPCC'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 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 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 by the line manager 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 to see.

- The manager informs the parent that the file is now ready and invites him/her to make an appointment to view it.
- The manager and a colleague will meet with the parent 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 legal representative or interpreter.
- 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 our Complaints Procedure.
- 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.

Never 'under-record' for fear of the parent seeing, nor should they make 'personal notes'.

Transfer of records

Records about a child's development and learning in the EYFS are made by our Care and Education settings and across our community services; 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 designated person's responsibility to ensure that records are transferred and closed in accordance with the archiving procedures, set out below.
- If the Local Safeguarding Partners (LSP) retention requirements are different to the setting, the designated person will liaise with their line manager, and seek legal advice if necessary.

Development and learning records

- A team member 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 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 summary shared with schools should also include whether the child is in receipt of, or eligible for EYPP or other additional funding.
- The record contains a summary by the key person and a summary of the parents' view of the child.
- The document may be accompanied by other evidence such as photos or drawings that the child has made.
- The assessment summary should be completed and shared with the parent 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 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 person should make decisions on a case by case basis, seeking legal advice as necessary.
- The designated 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 can request that any factual inaccuracies are amended prior to transfer.
- 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 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 person will seek legal advice.
- In the event that LSP 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.

- 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.
- Prior to sharing the information with the receiving setting the designated person 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 person's line manager, who will agree how to proceed.
- If a child protection plan or child in need plan is in place a 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.
- Where a CAF/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, or after the information has been encrypted.
- Parent/carers should be made aware what information will be passed onto another setting via our '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 DSL must review and update Child welfare and protection summary, checking for accuracy, proportionality, and relevance, before this is copied and sent to the setting/school.
- The DSL 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 files

- Paper documents are archived with the child's name and date of birth on the front and the date they left and the length of time the file should be kept before destruction (Care and Education only). All paperwork is sealed and placed in an archive box and stored in a safe place i.e. a locked cabinet for a minimum of three years or until the next Ofsted inspection conducted after the child has left the setting, and can be destroyed following our retention period chart.
- For web-based or electronic children's files, 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 in line with required retention periods.

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 Sept 23)
- Data Protection Act 2018

Further guidance

- Working Together to Safeguard Children (DfE 2018) 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 2018) www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice

- 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

Policy Name	Data Protection and Information Sharing
Version Number	V3 of new format
This policy was developed by	Governance Group
These people were consulted/ involved in developing the policy	Data Protection Leads Senior Leadership Team Safeguarding Team Pre School Learning Alliance LBWF Governance group
This Policy was adopted by	Trustee Board
Date	September 2023 – extended to December 23
Signed	Bisi Oyekanmi
Name	Bisi Oyekanmi
Role	Chairperson
Next Review Date	September 2024