

# Information and Records

## Data protection

### Intention

This policy sets out how and why Handsworth Pre-School collects and processes data; and how privacy is maintained. It includes the procedures for managing subject access requests; managing and reducing the risks of data breaches; and how any breaches will be managed. It also includes information about third parties with whom data is shared.

Personal data is defined as any information that can identify the person concerned. It covers all data regardless of whether it is on paper or in an electronic format. It also includes pictures or images of individuals.

### The Legal Framework

- General Data Protection Regulations (GDPR) 2018
- Data Protection Act (DPA) 2018
- Early Years Foundation Stage (EYFS) 2020
- Special Educational Needs Code of Practice 2014 and Working Together to Safeguard Children 2015

### Scope

This policy applies to all data collected held on children, parents and families<sup>1</sup>, staff, trustees, volunteers, visitors or other individuals with whom the Pre-School works.

It links to the following other policies:

- Children's Safety and Security
- Maintaining Health and Safety at Pre-School
- Managing Health Care Needs
- Protection of Children from Abuse
- Safer Recruitment and Staffing
- Student Placements and Volunteers
- Supporting Children with Special Educational Needs
- Admissions
- Curriculum, Teaching and Learning
- Parental Involvement and Behaviour
- Parental Complaints
- Staff Complaints and Whistleblowing
- Terrorism and Lockdown

---

<sup>1</sup> Throughout, "parents" refers to parents and carers including legal guardians. "Families" refers to wider family members or friends who may be named as contacts on a child's Registration Form, given authorisation to collect a child or otherwise give parents permission to share their contact details with the Pre-School in line with relevant policies.

## **Compliance**

All staff, volunteers, trustees and committee members must comply with this policy and the procedures set out in the Appendices. Compliance is a condition of employment; or of taking up any voluntary role. Any deliberate breach of this policy will result in disciplinary action for staff. This may include dismissal and/or legal action if appropriate. If a volunteer deliberately breaches this policy, they will be asked to step down from their role and legal action may be taken if necessary.

All adults who work or volunteer at Pre-School must maintain a confidential relationship with each other and with the families and children at Pre-School. The privacy of children and their parents and carers must be respected.

## **Implementation: Roles and Responsibilities**

The **Pre-School Committee** has overall responsibility for ensuring compliance with legislation.

The **Data Policy Lead** is: Pre-School Leader, Janet Cushing

The **Data processor** is: Business Manager, Ruth Mattison

**All staff** are responsible for:

- Collecting, storing and processing personal data in accordance with this policy
- Informing the Pre-School of any changes to their personal data
- Contacting the Policy Lead if:
  - They have any questions about this policy or data collection, storage or use
  - If they are unsure about how or whether they may collect, use or keep any personal data they have been given
  - If there has been a data breach
  - If they want to find out about the data that is collected, used or stored on themselves as the data subject

## **Why Data Is Collected**

The Pre-School is legally required to collect, hold and share some data, as set out in the legislative and policy framework above.

Some data is collected, held and shared in order to fulfill contracts. This includes, amongst others, the contract we hold with the Local Authority to deliver early years education, and with individuals as members of staff.

The majority of the data we collect, hold and share is done with the clear, informed consent of individual(s) and parents concerned. Consent is not assumed and can be withheld or withdrawn.

## **What and How Data Is Collected**

The Asset Register provides a detailed list of the data collected, stored and processed by the Pre-School. A summary of the main areas of data we collect is below:

<p>Data on Children</p>	<ul style="list-style-type: none"> <li>• Registration Forms</li> <li>• The daily register, advised absences and collection forms</li> <li>• Medical Forms including Health Care Plans</li> <li>• Special dietary needs form</li> <li>• Tapestry learning journals</li> <li>• Accident or Incident Records</li> <li>• Safeguarding Records, Child Protection or Child in Need Records. Copies of documents to confirm formal Guardianship or Adoption of child.</li> <li>• Special Educational Needs and Disability support plans; records of reports from other professionals and/or Education Health Care Plans (EHCPs)</li> <li>• Financial records including fee payment; Free Early Education Entitlement Grant (FEEE) funding forms. Copies of forms of identification (passport, birth certificate,) as required by the Local Authority to verify funding.</li> <li>• Images and voice</li> </ul>
<p>Data on Parents and Families</p>	<ul style="list-style-type: none"> <li>• Child Registration Forms</li> <li>• Child Medical Forms including Health Care Plans</li> <li>• Tapestry learning journals</li> <li>• Child Safeguarding Records, Child Protection or Child in Need Records. Copies of documents to confirm formal Guardianship or Adoption of child.</li> <li>• Copies of legal constraints placed on an adult with parental responsibility, if appropriate</li> <li>• Child Special Educational Needs and Disability support plans; records of reports from other professionals and/or Education Health Care Plans (EHCPs); Local Authority sharing of information consent forms, in respect of SEND.</li> <li>• Financial records including fee payment; Free Early Education Entitlement Grant (FEEE) funding forms. Copies of forms of identification (household bills) as required by the Local Authority to verify funding. FEEE funding forms may require us to hold information about the benefits received, household income, and parents' national insurance numbers.</li> <li>• Records of complaints made through the Parental Complaint Procedure.</li> </ul>
<p>Data on Staff and Volunteers</p>	<ul style="list-style-type: none"> <li>• Application and interview for the role</li> <li>• Contract of Employment</li> <li>• Records of attendance and absence</li> <li>• Records of and sufficient to take forward background checks performed through the Disclosure and Barring Service</li> </ul>

	<ul style="list-style-type: none"> <li>• Records of performance recorded through supervisions, appraisals, or work-related meetings. Records of disciplinary procedures</li> <li>• Records of staff meetings, INSET or planning meetings.</li> <li>• Records of pay, pensions, taxation and benefits</li> <li>• Health and welfare including accident records, medication, and medication conditions. This may include reports from other professionals shared with consent by staff members. Records of next of kin.</li> <li>• Records of safeguarding or welfare concerns, whistle-blowing or complaints</li> <li>• Records of discussions with other agencies or professionals (for example, SEND reviews, EHCP meetings, CIN or CP meetings etc.).</li> <li>• Images and voice</li> </ul>
Data on Pre-School Trustees	<p>As for Parent Data and including also:</p> <ul style="list-style-type: none"> <li>• Records of and sufficient to take forward background checks performed through the Disclosure and Barring Service</li> <li>• Records enable the Pre-Schools ongoing registration with the Charity Commission and OFSTED</li> <li>• Bank details, if shared with the Pre-School Treasurer/Business Manager, in order to have expenses paid directly.</li> <li>• Records in minutes of meetings or be recorded in discussions at Committee Meetings; or appear in accounting records.</li> <li>• Records of participation in Complaints or Whistle-blowing procedures</li> </ul>
Data on Visitors	<ul style="list-style-type: none"> <li>• As held in the Visitor's book.</li> <li>• Additional contact details such as email address as held for the purposes of further professional discussion in relation to SEND, Child Protection etc.</li> </ul>

### **Using and Sharing Data, Confidentiality and Privacy**

Privacy Notices inform parents, staff, trustees, volunteers, and others about the data the Pre-School collects, processes and shared. The privacy notices are available on the Pre-School website; and are given to parents, staff, volunteers, and others. They are kept up to date and reviewed regularly in parallel with this policy.

## **Children and Parents**

Personal information about a child will only be requested from or shared with the adults who are identified as having parental responsibility or guardianship on the Registration Form.

Data can only be withheld from an individual with parental responsibility if there are legal constraints in place.

Informed consent from parent(s) will be sought prior to sharing information. If there is a dispute between parents about whether data may be shared, Pre-School will meet with the parents individually or together to discuss the reasons for sharing the data. If the dispute between parents cannot be resolved at that point, and it is in the best interests of the child for data to be shared, the informed consent of one parent named on the registration form will be taken.

Data may be shared with statutory authorities without parental consent if seeking consent would endanger the child, a parent, or staff member.

Some parents choose to share personal details or data amongst themselves. Pre-School cannot be held responsible for information shared in this way

At public or open events parents and others are asked only to take pictures of their child. If other children appear in the background, we ask that these images are not shared on social media. The response to data breaches of this kind is set out in the Appendix 3.

Further information about managing risks around children's images is set out in the Safeguarding: Protecting Children from Abuse Policy.

## **Staff and Volunteers**

Personal information on staff will be sought from the staff member themselves and is shared with their informed consent. Data is shared with those who need to know, in general the Pre-School Leader (line manager) and Business Manager. Some data may be shared with the Chair of the Committee and named Trustees to meet legal requirements, or as part of contract or pay reviews. With consent, staff names and email addresses are loaded onto Tapestry (see below).

## **Trustees and Visitors**

Personal information on Trustees will be sought to maintain our registrations with the Charity Commission and with OFSTED. Personal data will be shared with these authorities as required on registration or re-registration. Consent is sought to share other personal data such as email addresses with the Pre-School Leader and Business Manager to maintain the operation of the Pre-School.

Personal data of visitors is given when signing the Visitors Book. Such data will be shared with their employer, statutory authorities and/or emergency services if requested or if there are safety, welfare or safeguarding concerns

## **Sharing Data with Third Parties**

### **Statutory or Government Agencies**

Data may be shared online via government secure websites, such as the Capita Recruitment and Vetting Service, the Local Authority portals for funding and Pupil Premium eligibility, OFSTED and the Charity Commission online registration and reporting forms. Some data may be shared via online reporting forms with the Health and Safety Executive or other government bodies, to record accident, incident or safeguarding information.

### **Private Companies**

Consent is sought to upload some personal data to Tapestry (The Foundation Stage Forum Ltd) in order to maintain children's learning journals. Tapestry has in place strict security and confidentiality arrangements. Details of Tapestry's security arrangements can be found here: [Security | Tapestry UK](#); and information about their data and privacy arrangements, including further data sharing with App providers, can be found here: [Privacy Policy | Tapestry](#).

Consent is sought to share some staff data with our payroll processor Paybureau. Information on their data and privacy compliance can be found in their contract with the Pre-School.

### **Sharing Data Without Prior Consent**

There may be occasions when data is shared without an individual's informed consent. This will be done if:

- We are advised, instructed or legally required to do so by the police or other statutory agency;
- We judge it to be in the best interests of the individual, including children, in an emergency situation or when engaging with the emergency services;
- We judge that prior consent will endanger or significantly or immediately threaten a child's health, safety or wellbeing, in line with legislation on Prevent and on protecting children from abuse; and/or
- We judge that prior consent will endanger or significantly or immediately threaten an adult's health, safety or wellbeing, in line with legislation on Prevent, safeguarding and health and safety legislation.

### **Sharing Without Consent: Anonymised Data**

The Pre-School is sometimes asked to share data with the Local Authority, OFSTED, Department for Education or other statutory body, or as part of research schemes. Data that is fully anonymised – in that it does not or will not identify an individual when shared – will be shared without prior consent.

### **Transferring Data**

If an individual requests that we transfer their data outside the country, we will do so in accordance with data protection law in place at the time.

### **Automated Processing of Data**

The Pre-School does not undertake automated processing of data although third party partners may do so. The third parties that the Pre-School works with, and information about their data and privacy arrangements, are set out above.

### **Updating, Amending or Removing Data**

The law requires that the information held is accurate and up to date. Individuals have the right to request that their data is amended or, in certain circumstances, removed.

Parents must inform Pre-School of any changes to their or their child's personal data.

Returning parents are asked to review and update the information provided on the registration form each academic year.

Staff must inform Pre-School if their personal data changes. They are asked once a year to disclose any changes to their personal information or to that of their family that may result in disqualification or disqualification by association.

The Pre-School must by law ensure that any medication taken by staff does not impair their ability to work with children. All staff are asked annually to provide an update on medication for this purpose. If they change or start new medication subsequent to the annual declaration, staff may be asked on a case-by-case basis to provide information and/or confirmation from a doctor/medical professional of the impact of the medication on their ability to work with children

Some of the data held may be professional judgement, for example, developmental reviews and reports on children. We reserve the right not to change judgments based on evidence and professional knowledge. Should the parent seek to contest this information, we will record the difference of view held by the child's parent. If necessary, parents will be referred to the Complaints Procedure.

Data will not be amended or removed if doing so will undermine a child's physical or mental health; and/or their safety or welfare. Data will not be amended or removed if doing so will undermine or damage the mental or physical health; and/or safety or wellbeing of staff or adults volunteering with us.

## **Subject Access Requests**

Parents have the right to ask to see the personal information that we hold about them and their child. Staff and other adults have the right to see the personal information we hold about them. To do so, individuals must make a subject access request. The procedure is set out in Appendix 2.

## **Data Security: Minimising Risk**

Paper or electronic files may be stolen or mislaid. Computer files may be hacked. There is a risk of burglary from the premises when Pre-school is closed. There is a risk that other members of the Pre-School (parents and family members, trustees, volunteers and visitors) maliciously access the personal data of others. There is a risk that other users of the Hall access Pre-School data accidentally or on purpose.

To manage these risks, staff must:

- Ensure that data is only accessible or available to staff members who have a professional need to see it
- Ensure that all personal data is put away and stored securely at the end of each session
- Check that filing cabinets are locked at the end of each session.
- Check that the storage cupboard and storage room are locked at the end of each session
- Check that all personal data that may be displayed during session time (e.g. dietary requirements) is securely packed away.
- Ensure that displays, the website and Tapestry only display images of children where parental consent is given. Images of children where parental consent is withheld or withdrawn are not on display.
- Ensure that images on the closed Facebook Group are do not include children's faces or names, excepting when specific, advanced parental permission has been given for specific occasions.
- Ensure that any children's records of work which are transported are carried in a bag, kept secure at home and returned to the setting the following day.
- Ensure electronic equipment or files (e.g.: planning, reflections etc) are password protected
- Follow the Staff Code of Conduct on Using Tablets and the Internet

## **Disposal of Data**

Data is not held longer than necessary. The Asset Register sets out detail on how long data is retained. Paper files which identify individuals must be shredded. Electronic or digital files managed by staff must be deleted once a child leaves Pre-School or an adult leaves their role. Information on Tapestry is deleted in line with the program when children/staff members leave. Staff must return mobile devices to factory settings when they leave the Pre-School.

## Managing Data Breaches: Procedure

Appendix 3 sets out the procedure should a data breach be known or suspected.

The ICO, OFSTED and the Local Authority will be informed within 72 hours of any data breach where:

- Safeguarding information becomes available to unauthorized person(s).
- Laptops or computers are stolen that contain un-encrypted personal data about pupils.
- Financial data becomes available to unauthorised person(s).

If theft or malicious activity is suspected or known, the Police and the Landlords (the Baptist Church) will also be informed.

## Training; Monitoring and Review.

All staff must comply with this policy and procedures. Not to do so may be considered a disciplinary matter. This policy is regularly reviewed and updated.

This policy was adopted at a meeting of	<b>Handsworth Pre-school</b>	name of setting
Held on	<b>30 November 2021</b>	(date)
Date to be reviewed	<b>29 November 2022</b>	(date)
Signed on behalf of the management committee		
Name of signatory	<b>Jonny Cooper</b>	
Role of signatory (e.g. chair/owner)	<b>Chair</b>	

## Appendix 1: Definitions

<b>Term</b>	<b>Definition</b>
<b>Personal data</b>	Any information relating to an identified, or identifiable, individual.
<b>Special categories of personal data</b>	<p>Data that is more sensitive and so needs more protection. At Pre-School this may include information about an individual's physical or mental health.</p> <p>The law defines other areas of special category information. These other areas are an individual's race or ethnic origin; political beliefs; religious or philosophical beliefs; trade union membership; and sex life or sexual orientation. At Pre-School we would not expect routinely to collect or use data in these categories. We would however seek some or any of this information if we consider that not doing so would put children or other adults at risk of harm.</p>
<b>Processing</b>	Anything done to use the data or information provided. Processing data at Pre-School is generally done manually although some aspects of our data is processed automatically via government or Local Authority websites.
<b>Data subject</b>	The identified or identifiable individual whose personal data is held or processed.
<b>Data Policy Lead</b>	The person who determines the purpose and means of processing the personal data.
<b>Data processor</b>	A person or other body who processes personal data on behalf of the data policy lead.
<b>Data breach</b>	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.
<b>Asset register</b>	A list setting out what data we collect, why we collect it, how it is used, how it is shared and how long it is kept for (retained).

## Appendix 2: Procedure – Subject Access Requests

Requests **must**:

- be made in writing to the Pre-School Leader;
- include the name of the individual making the request, and the name of the subject of the request if different. We will only provide information about a child to those with parental responsibility. We will only provide information about adults to the individual concerned;
- include the address, telephone number and email address, as appropriate, of the person making the request; and
- detail the information being sought.

The Pre-School Leader will acknowledge the request in writing.

The Data Processor will prepare a file within 30 working days of the request being acknowledged. If the information request is complex or numerous, this timescale may be extended. If this is necessary to do so, the individual making the request will be informed within 30 working days. We will explain why it is necessary to extend the timescale and provide a new timescale for the delivery of the information.

There will be no fee or charge made.

Information will **not** be disclosed either wholly or partially if it:

- Might cause serious harm to the physical or mental health of a child, another child, a member of staff or another adult volunteering at Pre-School;
- Would reveal that a child is at risk of abuse and/or where the disclosure of information would not be in the child's best interests;
- Is contained in adoption or parental order records;
- Is given to a court in proceedings concerning a child or an adult at Pre-School.

Where information disclosed may include personal data of third parties, we will write to the third party seeking permission to share data. Third parties may include, but is not limited to:

- All adults named on forms, where information on that form is requested
- Other professionals named in reports, records etc, where that information is requested
- Other staff or adults who volunteer with Pre-School are named in reports, where that information is requested

Where third parties refuse consent to share their data, references to them will either be deleted or documents removed entirely.

Where data has been provided for the purposes of sharing with statutory or other agencies, such as the Local Authority; Capita/DBS etc, information will be provided that is held or used by Pre-School. Individuals can make subject access requests to the other agencies if appropriate.

Where data may be held by outside professionals or agencies about the individual, information held by Pre-School will be provided. Individuals may make subject access requests directly to the outside agencies/professionals. This may be relevant, for example, when assessments and reports have been made for a child who has or may have special educational needs.

Following a subject access request, data files will be shared with the individual on receipt of two forms of identification, including one picture identification.

The files will be handed directly to the individual making the request, in a sealed envelope. If this is not possible, the file will be posted to the address given in the original request using recorded and tracked delivery.

Subject to the nature of the information requested, a meeting with the individual may be requested. Individuals may bring up to two supporters to the meeting. Names of attendees must be provided at least 48 hours in advance of a meeting. Pre-School reserves the right to refuse entry if names are not provided in advance; and/or if we believe any attendee may be threatening or abusive to staff. Written notes of the meeting will be made.

Requests that are unfounded, excessive or repetitive (asking for further copies of the same information) will not receive a response.

Individuals will be informed if their request is refused or if information is withheld from a file. Individuals have the right to complain under the Parental Complaints Procedure or via the ICO if they are not content with the Pre-School's response to their subject access request.

We will record all subject access requests made; and our response. Information about subject access requests will be held for the lifetime of the Pre-School.

### **Appendix 3: Data Breach Procedure**

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Data Lead (DL). She will liaise with the Data Processor (DP) (Business Manager, Ruth Mattison).
- The DP will investigate the report and determine whether a breach has occurred. To decide, the DP will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorised people
- The DP will alert the Pre-school Leader and the Chair of the Parent Committee.
- The DP will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members where necessary.
- The DP will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DP will work out whether the breach must be reported to the ICO, Ofsted and/or the Local Authority. This must be judged on a case-by-case basis. To decide, the DP will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO, Ofsted and/or the Local Authority.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions will be kept on data protection files for the lifetime of the Pre-school.

- Where the ICO, Ofsted and/or the Local Authority must be notified, the DP will do this via the ‘report a breach’ page of the ICO website within 72 hours. As required, the DPO will set out:
  - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
  - The name and contact details of the DP
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DP will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DP expects to have further information. The DP will submit the remaining information as soon as possible
- The DP will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DP will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DP
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DP will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DP will document each breach, irrespective of whether it is reported to the ICO, Ofsted and/or the Local Authority. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on data protection files and kept for the lifetime of the Pre-School.

The DP and the Pre-school Leader will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

### **Minor data breaches.**

Sometimes data may be lost or shared accidentally. The most likely circumstances of minor data breaches and our responses are set out below:

- i) Information left unsecured after the setting has closed.
  - Staff will attempt to retrieve and secure the data as soon as possible.
  - Staff will determine whether others may have seen the data whilst it was unsecured.
  - If others may have seen the data, they will be contacted to confirm.

If they have seen the data:

- They will be asked to confirm in writing that they have not copied it/and/or that copies will be destroyed; that the data will be used or shared further.

ii) Data accidentally emailed to the wrong recipient:

- Sender will attempt to retrieve the email.
- If unsuccessful, the DP will contact the recipient of the email and ask that it is deleted, not shared, published, saved or otherwise used. The DP will seek written confirmation that this has been done.
- If misdirected emails are received, the recipient or our DP will
  - Contact the sender and/or their DP.
  - Delete the email.
  - Confirm in writing that this has been done and that the data has not been shared, copied, saved or otherwise used.

iii) Misdirected mail:

- Mail addressed to another setting but delivered to us in error will not be opened. We will contact the setting concerned and ask them to collect the letter or we will deliver it to them.
- Mail addressed to us but concerning children not on our register.
  - We will contact the sender and inform them that the letter is mis-addressed.
  - We will return the letter to the sender with written confirmation that we have not copied, used or saved the data.

iv) Images of children who are not theirs are published on social media inadvertently by parents.

- As soon as we are aware of the potential breach of confidentiality, we will contact the parent who has made the post and ask them to delete it.
- We will inform the parents of the other children concerned that this has happened.

v) Parents post on social media about children and/or behaviour they have observed in the setting; or staff.

- As soon as we are aware of the potential breach of confidentiality, we will contact the parent who has made the post and ask them to delete it.
- We will inform the parents of the other children concerned that this has happened.
- We will also inform staff concerned that a breach of confidentiality may also have occurred.