

# Information and Records

## Data protection

### 1. Policy Statement

Handsworth Pre-School aims to ensure that all personal data collected about staff, children, parents, trustees and committee members, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR).

Personal data is defined as any information we collect 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 of individuals.

### 2. The Legal Framework

**Data:** This policy has been updated to meet the requirements of the GDPR and the DPA (2018). We have also taken into account guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice on subject access requests. We have taken into account guidance from the Pre-School Learning Alliance (PSLA) on the GDPR and on document retention requirements.

**Children's Records:** We have taken into account the requirements of the Early Years Foundation Stage 2017 (EYFS) as the basis for the data we collect, store and process on children and their families who apply to and attend Pre-School.

For children with special educational needs or where we have safeguarding concerns, we have also taken into account the requirements set out in "Working Together to Safeguard Children 2015" and "The SEN Code of Practice 2014".

**Staff, Trustee, Committee Member, Volunteers and Visitors:** We have taken into account the data requirements applicable to adults in the Pre-School as set out in the EYFS; as required by OFSTED to maintain our registration; as required by the Local Authority; as required by the Charity Commission to maintain our registration; and other data requirements set out to meet financial, accounting and health and safety legislation.

### 3. Compliance

All staff, volunteers, trustees and committee members are expected to comply with this policy. 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.

## 4. Definitions

Term	Definition
<b>Personal data</b>	Any information relating to an identified, or identifiable, individual.
<b>Special categories of personal data</b>	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.  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.
<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).

## 5. Roles and Responsibilities

The Parent Committee has overall responsibility for ensuring that Pre-School complies with all relevant legislation.

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

Our **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

## 6. Data Protection Principles

The GDPR sets out data protection principles with which we must comply. Personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfill the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Not kept for any longer than necessary for the purpose for which it is collected or used
- Processed in a way that ensures it is appropriately secure

The GDPR also sets out six ‘lawful bases’ (reasons) for processing personal data. At Pre-School we seek generally only to collect data that we are **legally required** to do so, under the legislative framework set out in Section 2 above. We may also collect data 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.

There are other areas under which we can process data. These include:

- **Vital interests** e.g.: to protect someone’s life
- **Public interest** e.g.: in order to carry out our official functions
- **Legitimate interests** of the Pre-School as an organization, provided the individual’s rights are not overridden; and
- When clear **consent** has been freely given.

Under the GDPR, individuals have rights about how we process personal data. These rights are:

- To be informed about the data we collect and what we do with it
- To be allowed to see it after we have collected it
- To be able to request changes if the data is incorrect
- To remove data if we have no legal right to hold it
- In certain circumstances, to ask that information is not processed or is removed
- To ask that we take account of any objections to the data we hold and/or how it is processed
- To ask that we transfer personal data
- To ask that we do not use their data to make automated decisions

## 7. Data Protection by Design and Default: Privacy and Confidentiality

We consider all adults who work or volunteer with us will maintain a confidential relationship with each other and with the families and children at Pre-School. It is our intention to respect the privacy of children and their parents and carers, whilst ensuring they have access to high quality early years education and care.

We aim to ensure that all parents and carers know and understand why we are asking for personal data and what we will do with it. We also take steps to ensure that only those who need to see

personal data have access to it; and that, in general, data is shared with informed consent. Under the law, we are able to share personal data without consent if we have concerns about a child’s safety or welfare.

We will only seek personal information about a child from an adult with parental responsibility. Personal information about children, including their Early Learning Records, or any other developmental files will only be shared with the child’s parent(s). We may seek parents’ informed consent to share information, for example, with other professionals. We may share information without consent if we are concerned about a child’s safety or welfare.

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

We inform parents, staff, trustees, volunteers and others about the data we collect and process through published **Privacy Notices**. These 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.

**8. The Data we Collect and How we Use It**

To detail the information we collect, use and store, we have developed an **Asset Register**. We keep the Asset Register under regular review. A summary of the areas in which we collect, and process data is below:

Children’s Data:	Including, but not limited to: Name, date of birth and gender Early Learning Records (ELRs) and other developmental reviews and reports; If applicable, reports from other professionals which are held on file by us; SEND Support Plans and/or Education, Health and Care Plans; registers; medication and/or accident books; special dietary needs/allergies; interests, likes and dislikes; photographs.
Parents’/Family Data:	Including, but not limited to: Name, address and contact details of those with whom the child lives and who have parental responsibility. The names of others who are important in the child’s life; Emergency contact details of other adults and/or of those who are authorised to collect your child from Pre-School. National insurance number(s); and copies of documents required by the Local Authority to confirm identification for the purposes of claiming grant funding. This may also include some information about benefits and/or household income. Information about your child and family’s ethnicity and cultural background (if given).

<p>Staff Data:</p>	<p>Including, but not limited to:</p> <p>Name, address, telephone numbers, date of birth, gender, qualifications and work history and copies of documents confirming these details.</p> <p>National insurance number; bank details and information about pay, taxation, pensions and benefits as appropriate.</p> <p>Information confirming background checks including enhanced criminal records checks (DBS); and references (as appropriate)</p> <p>Information about health, medication and medical conditions. This may include reports from other professionals which are held on file. This may include dietary needs/allergies.</p> <p>Accident records, including those required by the Control of Substances Hazardous to Health (COSHH) regulations.</p> <p>Records of attendance and absences.</p> <p>Any information recording any safeguarding concerns; Whistleblowing or Complaints.</p> <p>Copies of job application forms including Curriculum Vitae and other supporting documents. Records of interviews and assessments.</p> <p>Records of staff supervisions, appraisals or other work-related personnel meetings.</p> <p>Information relating to any disciplinary and/or grievance procedures.</p> <p>Information about training undertaken whilst employed by Pre-School.</p> <p>Records of general staff meetings, INSET days, planning meetings etc; and have been recorded as undertaking actions from our Improvement Plan or outcomes from audits or inspections.</p> <p>Records of discussions with other agencies or professionals (for example, SEND reviews and EHCP meetings; safeguarding reviews etc).</p>
<p>Trustee Data:</p>	<p>Including, but not limited to:</p> <p>Name, date of birth and gender; address, telephone number, email address and other relevant contact details</p> <p>National insurance number; and copies of documents required to confirm your identity and to initiate enhanced criminal records checks (DBS)</p> <p>Background; criminal records, convictions, court orders, reprimands, warnings or cautions etc as required to complete DBS checks.</p> <p>Bank details, if shared with the Pre-School Treasurer, in order to have expenses paid directly to you.</p> <p>References in minutes of meetings or be recorded in discussions at Committee Meetings; or appear in accounting records.</p> <p>Complaints; or Whistleblowing records.</p>
<p>Volunteer and Visitor Data:</p>	<p>Including, but not limited to:</p> <p>Name, address, telephone numbers, date of birth, gender, qualifications and work history and copies of documents confirming these details.</p> <p>Details of next of kin and emergency contact details</p> <p>Information confirming background checks including enhanced criminal records checks (DBS); and references (as appropriate)</p> <p>Records of health, medication and medical conditions and/or any information you give us about dietary needs/allergies.</p>

Accident records, including those required by the Control of Substances Hazardous to Health (COSHH) regulations. Records of your attendance and absences (if appropriate: for example, for work experience) Any information recording any safeguarding concerns; Whistleblowing or Complaints.
--

**Photographs:** We may take photographs of children or others at Pre-School. We obtain written consent from parents to take and to use photographs of their children. Adults are asked for their permission at the time the picture is taken. Consent can be withheld or withdrawn at any time. When using photos, children are not named.

When we hold open events to which parents, carers and others are invited, we ask all concerned to be careful only to take pictures of their child. We also ask that if pictures taken include images of other children, in the background, for example, these photographs are not shared or published on social media.

We set out more information in our Safeguarding: Protecting Children from Abuse Policy about how we manage safeguarding risks around taking and using photographs.

## 9. Updating, Amending or Removing Data

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

Parents are asked to inform Pre-School of any changes to their, or their child's, personal data. In particular, it is important that contact details provided on the registration form are kept up to date.

Parents are asked at least once per year to review and update the information provided on the registration form.

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 if this may result in disqualification or disqualification by association.

We are required by law to ensure that any medication taken by staff does not impair their ability to work with children.

Some of the data we hold may be professional judgement, for example, developmental reviews and reports on children. We reserve the right not to change our judgements, if they are based on professional knowledge and evidence. Should the parent seek to contest this information, we will record the difference of view held by the child's parent. If necessary, we will refer the parent to our Complaints Procedure; and/or seek legal advice.

We will also not amend or remove data if we think that doing so will undermine a child's physical or mental health; and/or their safety or welfare. Similarly, we will not amend or remove data if

we think that doing so will undermine or damage the mental or physical health; and/or safety or wellbeing of staff or adults volunteering with us.

## **10. Sharing Data**

Our Asset Register details with whom data is shared. We have to share some data with other agencies in order to comply with the law or meet our contractual obligations. Where we collect data that will be shared, we normally make this clear. We are also required to share data with or without consent if we are concerned about a child's safety or welfare.

We will also share data with law enforcement and government bodies where we are legally required to do so. For example:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Research and statistical purposes, where data can be sufficiently anonymised or consent has been provided.

We may also share personal data with emergency services and/or local authorities to help them respond to emergency situations; or if we are concerned about the health or welfare of a child.

Where we are asked to transfer data outside the country, we will do so in accordance with data protection law.

Some data is shared with government websites, for example, the Capita Recruitment and Vetting Service which processes the enhanced criminal records checks (DBS); the Local Authority 'online checker' for Pupil Premium eligibility etc.

Where data is shared with other third parties, for example, or our payroll processor, we take steps to ensure that the data will be processed and held securely in accordance with the GDPR and the law.

## **11. Subject Access Requests**

Parents have the right to ask to gain access to the personal information that we hold about them and their child. Staff and other adults have the right to gain access to the personal information we hold about them.

Individuals making 'subject access requests' must follow the procedure set out below.

## **Procedure:**

### 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 it 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.

We will **not** disclose information 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, we will either delete references to that third party within documents or remove documents entirely.

Where data has been provided for the purposes of sharing with statutory or other agencies, such as the Local Authority; Capita/DBS etc, we will provide the individual with the information 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, we will provide only the information we hold on file. 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.

When returning the data file to the individual who has made the request we will:

- Ask for two forms of identification, including one picture identification.
- Hand the information 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, we may meet with the individual to discuss the information we are providing. 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.

We will not respond to requests if they are unfounded or excessive; or if it is repetitive (asking for further copies of the same information).

If we refuse requests completely; if information is withheld from a file, we will tell individuals why. If individuals are discontent with the information we have provided or with our refusal to provide information, they have a right to complain to Pre-School, using our Complaints Procedure; and/or to the ICO.

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.

## **12. Data Security and the Secure Disposal of Data**

We are required by law to ensure that personal data is accessible and available only to those who have a professional need to see it.

Paper files are held in lockable filing cabinets in the cupboard in the Pre-School hall. The cupboard is locked at the end of the session. Only Pre-School staff know the combination of the lock. Data held on computer is password protected.

We do not keep data for longer than it is needed. Our Asset Register sets out detail on how long data is retained. When we destroy or remove data, paper files are shredded; and any electronic files are deleted.

## **13. Data Breaches**

We will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected personal data breach, we will follow the procedure set out in Appendix 1.

If appropriate, we will inform the ICO, OFSTED and the Local Authority within 72 hours of the data breach if, for example:

- 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)

#### **14. Training; Monitoring and Review.**

All staff are trained in data protection.

All staff are expected to comply with this policy and not to do so may be considered a disciplinary matter.

This policy is regularly reviewed by staff and updated in line with the law and good practice.

This policy was adopted at a meeting of	<b>Handsworth Pre-school</b>	name of setting
Held on	<b>25 February 2020</b>	(date)
Date to be reviewed	<b>24 February 2021</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: Personal 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.

## **Managing the risk of data breaches**

We will take the action to mitigate the impact of data breaches, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

### **1. Significant data breach**

We will consider any loss of sensitive personal information to be significant. Also, any loss of large amounts of personal data in either paper or electronic form is significant. There is a risk that paper or electronic files may be stolen, in the case of data on computer, may be hacked. We are at risk of burglary from the Pre-school premises when Pre-school is closed.

We will take the actions set out in this policy to reduce the risk of data breaches in this way.

In addition, staff must:

- Check that filing cabinets are locked and secured at the end of each session.
- Check that the cupboard and `bunker` 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 at the end of the session.

When staff remove files from the Pre-school to work on at home, they must:

- Ensure files are transported securely.
- Minimise risk of others seeing personal data by tidying files away and ensuring other family members do not access personal data.
- Return files to the setting the following day,
- Ensure electronic files are password protected.

If a data breach occurs, we will follow the procedure set out in this policy.

### **2. Minor data breaches.**

Whilst we take steps to ensure data is secure, we know that 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 Pre-School 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.