



Thamesview Confidentiality Policy & General Data Protection Policy

Early Years Welfare requirements

3.4-3.8 – Child Protection

3.67- Information and records

Key themes:

Unique Child

Positive Relationships

Enabling Environments

Statement of intent

We believe that all children and their families are entitled to personal and confidential services. All staff has a duty to respect confidentiality and to only disclose information on a 'need to know' basis.

- All staff at Thamesview have an individual responsibility to respect and maintain confidentiality at ALL times.
- Parents/carers should be made aware that confidential information will not be shared with other staff or agencies unless:
 - 1.1.1. The welfare of the child is at risk
 - 1.1.2. They can demonstrate the need to know

GDPA (General Data Protection Regulation).

Thamesview must comply and adhere to the GPRA (General Data Protection Regulation).

Members of Thamesview (parents/carers/staff/children) may withdraw consent to hold information/data at any time – this can be requested through any staff member and organised by the setting manager.

Personal Data is defined as information relating to an individual, whether it relates to his or her private, professional or public life. It can be a name, photograph, postal address, email address, bank details, medical information, identification number, location data or online identifier.

The GDPR applies to the collection and processing of personal data on manual filing systems, electronic devices and systems, and posts on social media.

All paper work is securely stored and held for the required amounts of time as detailed below:

Retention Periods for Records:

Children's records	Retention Period	Status	Authority
Children's records- including registers, medication, book and accident records and books pertaining to the children	Records should be retained for a reasonable period of time (for example 3 years) after children have left the Provision	Requirement	Early Years Foundation stage welfare requirements (given legal force by Child care Act 2006)



	Until the child reaches the age of 21, or until the child reaches the age of 24 for child protection records	Recommended	Limitation Act 1980/The Statute of Limitations (Amendment) Act 1991. Normal limitation rules (which mean that an individual can claim for negligently caused personal injury up to 3 years, or deliberately caused personal injury up to 6 years after event) are postponed until a child reaches 18 years old
Records of any reportable death, injury, disease or dangerous occurrence	3 years after the date on which it happened	Requirement	The reporting of injuries, Diseases and Dangerous Occurrence Reaches 1995 (RIDDOR) (SI 1995/3163)
Personnel Records	Retention Period	Status	Authority
Personnel files and training records (including disciplinary records and working time records)	6 years after employment ceases	Recommended	Chartered Institute of Personnel
Application forms and Interview notes (for unsuccessful candidates)	6 months to 1 year	Recommendation	Chartered Institute of Personnel
DBS Check / Disclosure information	25 Years	Requirement	Criminal Record Bureau Organisations that are subject to Ofsted inspections are entitled to retain Disclosure certificate until the date of inspection, after which only the following basic information may be securely destroyed in line with the CRB Code of Practice. • The date of issue of Disclosure • The name of the subject • The type of Disclosure requested • The position for which the Disclosure was requested • The unique reference number of the disclosure • The details of the recruitment decision taken
Pay Records	Retention Period	Status	Authority
Wage / salary records (including overtime, bonuses and expenses)	6 years	Requirement	Taxes Management act 1970
Statutory Maternity Pay (SMP) records	3 years after the end of the tax years in which the maternity period ends	Requirement	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986 / 1960)
Statutory Sick Pay (SSP) records	3 years after the end of the tax year to which they relate	Requirement	The Statutory Sick Pay (General) Regulations 1982 (SI 1982 / 894)
Income tax and National Insurance returns / records	At least 3 years after the end of the tax year to which they relate	Requirement	The Income tax (Employment) Regulations 1993 (IS 1993 / 744



Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of redundancy	Recommendation	Chartered Institute of Personnel
Health & Safety Records	Retention Period	Status	Authority
Staff accident records (for organisations with 10 or more employees)	3 years after the date of the last entry (there are separate rules for the recording of accidents involving hazardous substances)	Requirement	Social Security (claims and payments) Regulations 1979 (SI 1979 / 628)
Records of any reportable death, injury, disease or dangerous occurrence	3 years after the date of which it happened	Requirement	The reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995 / 3163)
Accident/ medical records as specified by the control of Substances Hazardous to Health Regulations (COSHH) 1999	40 years from the date of the last entry	Requirement	The Control of Substances Hazardous to Health Regulations 1999 (COSHH) (SI 1999/ 437)
Assessments under Health and Safety Regulations and records of consultations with safety representative and committees	Permanently	Recommendation	Chartered Institute of Personnel
Financial Records	Retention Period	Status	Authority
Accounting records	3 years for private companies, 6 years for public limited companies. 6 years for charities	Requirement	Section 221 of the Companies Act 1985 Charities Act 1993 (c. 10) Part VI
More detailed information on retention of financial records is provided in Finance in Early Years Settings (Ref: A078) Pre-school Learning Alliance			
Administration Records	Retention Period	Status	Authority
Complaints record book	At least 3 years from the date of the last record	Requirement	Early Years Foundation Stage Welfare Requirements (given legal force by childcare Act 2006)
Insurance liability documents	40 years from date of issue	Requirement	The Employers' Liability (compulsory Insurance) Regulations 1998
Minutes / minute book	Permanently	Recommendation	Chartered Institute of personnel

Records	Length of time to keep
<u>Children's Records</u>	
Accident reports	21 years 3 months
Medical records	30 years
Parent contact details	2 years
Details about child	2 years
Outing permission	2 years
Permission to administer medicine	21 years 3 months
Emergency treatment permission	21 years
Collection authority	21 years



Incident reports	21 years
Register	21 years
<u>Staff records</u>	
All personal records	7 years
Individual wage slips	2 years
Time sheets	3 years
Accident reports	21 years
Staff attendance records	21 years
National insurance/tax income returns	7 years
Unsuccessful job application forms	4 months
Unsuccessful job interview records	4 months
<u>Insurance</u>	
Certificates	40 years
<u>Visitors</u>	
Record of visitors	2 years
<u>Licence or lease</u>	
Licensing agreement or lease	6 years
<u>Committee, students and volunteers</u>	
Personal details	2 years
<u>Committee records</u>	
Minutes of meetings and annual reports	6 years
Bank statements	6 years
Bank reconciliations	6 years
Remittance advice	10 years
Recipients cash balances	10 years
Sales ledgers	3 years
Correspondence re donations	3 years

The setting manager has undertaken GDPR guidance from SCC

Parents and staff all receive a privacy notice. This is also displayed on our 'policy page' on our website.

Individual Rights

The GDPR includes the following rights for individuals:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object;
- The right not to be subject to automated decision-making including profiling.

How personal data is deleted

- Who will make the decisions about deletion: - The setting manager(s).



- Personal information 'paperwork' will be shredded and destroyed appropriately.
- All ICT personal data will be permanently deleted from all systems as required.

The right to data portability only applies:

- To personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

Personal data shared electronically and in a commonly used format will be password protected.

Thamesview will not charge for complying with a request for copies of any personal data and will comply within one month. Thamesview will charge for requests that are manifestly unfounded or excessive. If a request is refused Thamesview must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. This must be done without undue delay and at the latest, within one month.

Information held

At Thamesview we hold children's, parents and carers personal information and data including contacts, emails, photos, DOB, SEN information and statistics, health information and personal data. This information is shared only with parents' permission or in line with setting policy, and then only with third parties relevant to the families we work with, for example;

- Health visitors,
- Doctors
- EYFS and SEND agencies,
- LA
- Schools
- Children centres.

Accountability Principle:

If inaccurate information is shared with another organisations Thamesview must correct its own records and information and inform the other organisation that the information provided was inaccurate.

Consent

Consent is sought from parents on their setting application forms and via our setting privacy notice.

Parents have the right to update information and data as required and at any time.

Thamesview have made the request for consent prominent and separate from our terms and conditions.

We ask people to positively opt in.

We use clear, plain language that is easy to understand.

We specify why we want the data and what we're going to do with it.



We have named our organisation and any third parties.

We tell individuals they can withdraw their consent.

We record consent. We keep a record of when and how we got consent from the individual.

We regularly review consents to check that the relationship, the processing and the purposes have not changed.

We have processes in place to refresh consent at appropriate intervals, including any parental consents.

We make it easy for individuals to withdraw their consent at any time and publicise how to do so. We act on withdrawals of consent as soon as we can. We don't penalise individuals who wish to withdraw consent.

Staff sign a consent form to share and use their personal data as detailed in our privacy notice.

Personal Data Breach

Thamesview are required to notify the ICO and the ERYC when they suffer a personal data breach. It is our duty to report certain types of data breach to the ICO, and in some cases, to individuals. Only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly.

It is the managers responsibility that there is no data breach and to effectively detect, report and investigate a personal data breach.

Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

Data storage and data security collecting new data or accessing existing data:

Hard copies such as interview notes, prints of photographs, child's profiles, application forms, or video/audio tapes are kept securely locked away – These are stored in our locked staff cupboard - they can only be accessed by agreed members of staff.

Staff confidential information is stored in a locked filing cabinet – accessed by the setting manager and deputy only.

Files - including computer files - that contain personal or identifiable data (such as names). These files are password protected, and only accessed by agreed members staff. Particular care must be taken if sharing files within the wider early years team that they have secure GDPR policies in place.

Data Protection Officer

(Lead practitioner who takes the lead on ensuring your setting is GDPR compliant).

Our Data protection officer is – SAMANTHA IRELAND



Third party information sharing

Thamesview must ensure that when information is shared with any third party, with permission, that they are compliant with the GDPR and they too are meeting the requirements of the GDPR and provide sufficient guarantees of this.

PRIVACY NOTICE: Thamesview Preschool

General Data Protection Regulation (GDPR).

Thamesview is a data controller for the purposes of the GDPR (General Data Protection Regulation). We collect information from you and may receive information about you from your previous setting, local authority and/or the Department for education (DfE). We process this personal data and use it to:

- Assist families by providing information to families to enable them to make a considered choice when accessing education.
- Provide appropriate support and pastoral care including access to relevant support services that may be required.
- To book courses, training and online learning.
- Improve services that impact on children's outcomes by assessing the data
- Monitor and report on children's progress and development.
- Apply for appropriate LA funding and support as required.
- The further use of any information will always be discussed with the parent/child and staff member before being shared.

All data must be freely given, specific and fully informed. Consent must also be revocable (people can withdraw their consent at any time) Procedures are in place to action and record this when this happens.

This information includes contact details, national curriculum assessment results, attendance information, family benefit information as it relates to EYPP (Pupil Premium) eligibility, housing,

information provided by the family / other agencies related to personal characteristics such as your ethnic group, any special educational needs, relevant medical information and details of services provided.

Who we share data with:

We will not give information about you to anyone outside this establishment without your consent unless the law and the school's policies permit it. We are required by law to pass some of your information to the Local Authority (LA) for monitoring, tracking and provision of appropriate services, to the Department for Education (DfE) and local children's centres. The LA and the DfE in turn are required to share some information with trusted partners including local NHS Trusts and other local authorities. Appropriate data will be used by certain Local Authority services to provide the best support possible to children and young people.

What will be the effect of this on the individuals concerned: -The data you provide will enable Thamesview to provide the best education and care for your child.



You have the right to log a complaint with the ICO about any data concerns.

Individuals may request a copy of the information held about them. Under the GDPR such requests will need to be responded to within one month. Information must be provided for free/no cost. If you want to receive a copy of the information about your son/daughter that we hold, please contact: Individuals maintain the right to change any data that is incorrect and maintain the right not to have it processed if they ask Thamesview

- SAMANTHA IRELAND , Setting Manager.

Thamesview Preschool, Manor Road, Walton on Thames Surrey KT12 2PH

thamesviewpreschool@outlook.com

Opt-in data consent:

Please sign and date (parent/carer) to confirm we 'Thamesview Preschool' can use your and your child's personal data provided as detailed in this Privacy notice.

FULL NAME: _____

SIGNED: _____ DATE: _____

Working Together to Safeguard Children.

This policy represents the agreed principles for confidentiality throughout the nursery. All setting staff and volunteers, representing Thamesview must agree to this policy.

Thamesview works with many children and families and sometimes will be in contact with confidential information.

Ensuring that children and young people are kept safe is vital. Where information sharing is necessary to achieve this objective, it is important that practitioners have a clear understanding of when information can be shared. It is also for them to understand the circumstances of when sharing is inappropriate.

We will respect confidentiality in the following ways:

- Parent will have ready access to the files and records of their own children but will not have access to information about any other child.
- Issues to do with the employment of staff whether paid or unpaid, will remain confidential to the people directly involved with making personnel decisions.
- Staff will not discuss the individual children, other than for purposes of curriculum planning/group management, with people other than the parent/carers of the child.
- Students on work experience or other recognised courses observing in Thamesview will be advised of our confidentiality policy and required to respect it.
- All the undertaking above is subject to the paramount commitment of the setting as is the safety and wellbeing of the child. Please see our Child Protection Policy.

The Data Protection Act is not a barrier to sharing information but is in place to ensure that personal information is shared appropriately.



At Thamesview we recognise that parents have a right to know that information they share will be regarded as confidential as well as be informed about the circumstances, and reasons, when we are obliged to share information.

We are registered with the ICO (information commissioner's office). – Data protection.

Definition: '*Confidential information is information of some sensitivity, which is not already lawfully in the public domain or readily available from another public source, and which has been shared in a relationship where the person giving the information understood it would not be shared with others.*' (Information Sharing: Practitioners' Guide).

At Thamesview, staff and managers can be said to have a 'confidential relationship' with families. It is our intention to respect the privacy of children and their parents and carers, while ensuring that they access high quality early years care and education in our setting.

We aim to ensure that all parents and carers can share their information in the confidence that it will only be used to enhance the welfare of their children. There are record keeping systems in place that meet legal requirements; means of storing and sharing that information take place within the framework of the Data Protection Act, the Human Rights Act and the EYFS (Early Years Foundation Stage).

Confidentiality Procedures

- We always check whether parents regard the information they share with us to be regarded as confidential or not. We ask parents if we can share information as appropriate (for example; developmental information regarding their child).
- Some parents sometimes share information about themselves with other parents as well as staff; the setting cannot be held responsible if information is shared beyond those parents whom the person has 'confided' in.
- Information shared between parents in a discussion or training group is usually bound by a shared agreement that the information is confidential to the group and not discussed outside of it.
- We inform parents when we need to record confidential information beyond the general personal information we keep (see our record keeping procedures) - for example with regard to any injuries, concerns or changes in relation to the child or the family, any discussions with parents on sensitive matters, any records we are obliged to keep regarding action taken in respect of child protection and any contact and correspondence with external agencies in relation to their child.

We are obliged to share confidential information without authorisation from the person who provided it or to whom it relates if it is in the public interest. That is when:

- It is to prevent a crime from being committed or intervene where one may have been or to prevent harm to a child or adult; or
- Not sharing it could be worse than the outcome of having shared it. •

The decision should never be made as an individual, but with the back-up of management committee officers. The three critical criteria are:



- Where there is evidence that the child is suffering, or is at risk of suffering, significant harm.
- Where there is reasonable cause to believe that a child may be suffering or at risk of suffering significant harm.
- To prevent significant harm arising to children and young people or serious harm to adults, including the prevention, detection and prosecution of serious crime.

Procedures

Our procedure is based on the 15 Points for Good Practice as set out in Information Sharing: Practitioners' Guide (HMG 2006)

- 1) Explain to families how, when and why information will be shared about them and with whom. That consent is normally obtained, unless it puts the child at risk or undermines a criminal investigation.
- 2) We ensure parents receive information about our information sharing policy when starting their child in the centre and they sign a form to say that they understand circumstances when information may be shared without their consent. This will only be when it is a matter of safeguarding a child or vulnerable adult. This is on our registration form.
- 3) We ensure parents have information about our Safeguarding Children and Child Protection policy.
- 4) We ensure parents have information about the circumstances when information will be shared with external agencies for example with regard to any special needs the child may have or transition to school.
- 5) Consider the safety and welfare of the child when making a decision about sharing information – if there are concerns regarding 'significant harm' the child's well being and safety is paramount.
- 6) We record concerns and discuss these with the setting's designated person and/or designated officer from the management committee for child protection matters. Record decisions made and the reasons why information will be shared and to whom.
- 7) We follow the procedures for reporting concerns and record keeping.
- 8) Respect the wishes of children and parents not to consent to share confidential information. However, in the interests of the child, we are able to judge when it is reasonable to override their wish.
- 9) Guidelines for consent are part of this procedure.
- 10) Managers are conversant with this and are able to advise staff accordingly.
- 11) Seek advice when there are doubts about possible significant harm to a child or others.
- 12) Managers contact children's social care for advice where they have doubts or are unsure.
- 13) Information shared should be accurate and up-to-date, necessary for the purpose it is being shared for and shared only with those who need to know and shared securely.
- 14) Our Safeguarding Children and Child Protection procedure and record keeping procedures set out how and where information should be recorded and what information should be shared with another agency when making a referral.



15) Reasons for decisions to share information, or not, are recorded.

At Thamesview we respect confidentiality in the following ways:

- Parents will have ready access to the files and records of their own children and no access to information about any other child.
- Issues to do with the employment of staff whether paid or unpaid, will remain confidential to the people directly involved with making personnel decisions.
- Staff will not discuss the individual children, other than for purposes of curriculum, planning, with people other than the parent/carers of the child.
- It is the responsibility of any staff member holding personal information to ensure that persons not allowed to view it cannot access it.
- Any telephone conversations regarding a child or family should be held in private to ensure that they are not overheard. In some situations staff may be asked to leave whilst a telephone conversation takes place.
- Records and files must not be left unattended i.e. on desks etc and must be locked in the filing cabinet or cupboard overnight.
- Permission must be sought from a manager to remove a file from the building, completing the signing in and out form in the office. The staff member removing the file must ensure the file is being transported safely and securely, never left unattended in cars overnight and kept securely in staff home. Journals are to be signed in when returning to Nursery.
- All staff, students and external professional that work at Thamesview have signed, respect and adhere to the confidentiality statement and policy.
- Staff are aware that any breach of confidentiality could result in disciplinary action.
- Staff should ensure that professional boundaries with families are maintained at all times. Staff must not form personal relationships with families outside of work or share personal information about themselves or others.

The Thamesview complies with the Data Protection Act 1998 & General Data Protection Regulations.

Legislation

Children Act 2006

Data Protection Act 2018

General Data Protection Regulation (**GDPR**)

Childcare Act 2006

UN Conventions on the rights of the child



Date of review: Jan 2024	Signature of Proprietors:
Date to be reviewed:	