FOUNDATION YEARS TRUST

INFORMATION MANAGEMENT POLICY

The Foundation Years Trust ("the Trust") stores information on children, families, nursery settings, staff (including volunteers and consultants) and Trustees as part of its work. How this information is collected, stored and shared is vital for the safety of children and families and the integrity of the Trust.

This policy covers:

- Data Protection
- Confidentiality and Information Sharing
- Record Keeping

DATA PROTECTION

The Trust is committed to the protection of the rights and freedoms of individuals in accordance with the provisions of the Data Protection Act 2018 (the Act) and the General Data Protection Regulation (GDPR).

The Trust is both a data controller and a data processor. This ensures we can effectively manage and measure the impact of our programmes and the administration of staff, trustees and volunteers.

The Trust ensures that all personal information is handled and dealt with properly howsoever it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means. All staff and volunteers with access to personal data are required to adhere fully to the Act and the GDPR in carrying out their duties for us.

The trustees have responsibility to ensure that this policy is implemented and appoint a data protection lead as the designated person with special responsibility for data protection in the Trust. The named Trustee is at the end of this document.

KEY FEATURES OF THE REQUIREMENTS WHICH INFORM THIS POLICY AND PROCEDURE

The Act relates to the processing of personal data and sensitive personal data which must be processed in accordance with the '*Six privacy principles of GDPR' (Schedule 2 attached)*.

The lawful basis for the data collected on the individuals and families we work with is "*consent*". This means that our service users have the choice to consent to share their data with the Trust.

An *individual's rights,* with reference to data protection, are the right to be informed; the right of access; rectification and to erase; the right to restrict processing; the right to object and rights in relation to automated decision making. The Trust adheres to the applicable individual's rights in its data collection and processing.

As a data controller, the Trust '*controller'* determines the purposes and means of the processing of personal data

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether that's by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Date policy was last adopted: 18 July 2019 Date of last review: 13 Nov 2020

Personal data is data which relates to a living individual who can be identified from data and other information which is in the possession of, or is likely to come in the possession of, the organisation and includes any expression of opinion about an individual.

Special category data is defined as personal data consisting of information as to racial or ethnic origin, political opinion, religious or other beliefs, trade union membership, physical or mental health condition, sexual life and criminal proceedings or convictions. Sensitive personal data has even greater conditions for processing and normally, to process the information, it will be necessary to have the explicit consent of the individual.

CONFIDENTIALITY AND INFORMATION SHARING

The Trust recognises that the proper use of confidential information underpins our service. All information about service users, staff, (including consultants and volunteers) and Trustees is treated as confidential, to be shared only in accordance with the Trust's agreed policy on information sharing.

1. PROCEDURES ON DATA COLLECTION AND PROCESSING

1a Service users

All service users who are accessing services provided by or paid for by the Trust are requested to complete a registration form. Details of the specific data collected are outlined in schedule 3.

Service users are asked for consent to allow the Trust to store, use and share relevant information to support the work of the programme. Consent also covers the sharing of information that is deemed necessary to meet the needs of the family.

Service users are aware of the purpose of the data collection and of their rights to withdraw that consent at any time or access data held on them.

Service users are informed that if they choose not to share their personal data, they are still able to access the Trust's services.

The condition under which the Trust collects special category data on ethnic origin is that of explicit consent. Service users are aware of their rights to withdraw this consent at any time.

Purpose of data collection

The Trust collects this data to understand the demographic of its service users; to monitor its services; to inform and improve its programme design and to evaluate the impact of its services.

Sharing information

Service users are informed that we do not disclose their confidential information outside the organisation without their explicit consent except*:*

- To protect the welfare of a child or adult at risk *or*
- In exceptional circumstances where a person is suspected of a disclosable offence[1] or terrorism.

Child protection, safety and welfare concerns will be recorded by the designated safeguarding people on the Trust's Record of Concern form. Information recorded will be factual, accurate and up-to-date and discussed with the recorder's line manager. See our Safeguarding policy for more information. The Trust will

[1] Disclosable offence: drug trafficking; drug money laundering

- Explain to service users at the outset how and when information on them will be shared
- Explain that information shared may relate to concerns if they arise, or information about children's progress. Consent will be obtained to share specific information relating to the family, the only exception being where there is a risk of significant harm to a child or serious harm to an adult.
- Wherever possible, however, the Trust will respect the wishes of children and families when sharing information about them.
- Ensure that the information shared is necessary for the purpose for which it is being shared, is shared only with those who need to see it and is accurate and up to date.
- Record the reasons for decisions to share or not share information in the family file.

Liaising with other agencies

The Trust is committed to maintaining effective communication with other key agencies and shares information according to these data protection principles, in order to contribute to the best support available for children and their families.

Multi-agency meetings

When invited, Trust staff will attend multi-agency meetings with the family's knowledge. When sharing information about a family it supports, the Trust adheres to the principle that the information is necessary, proportionate, relevant, accurate, timely and secure. When professionals unconnected with the family are present, Trust staff should emphasise the sensitive and confidential nature of the information they are sharing.

If providing reports for multi-agency meetings, the information provided about a family in a report is factual, accurate, up-to-date, substantiated or reflects a professional opinion and should be in writing.

1b Trustees

The information collected on Trustees is detailed in schedule 3. Trustees are made aware at induction that a record is held about them and that they have the right to request access to it, and that the file may be sampled by the Trustrees for quality-checking purposes.

Purpose of collecting data

Basic data on Trustees is collected upon joining the Board for administration and governance purposes.

Information sharing

Basic information on trustees is shared with The Charity Commission, Companies House and CAF Bank (if the Trustee is set up as a signatory).

The Trust will provide the Information Management Policy and procedures to all new trustees as a key part of their induction. All trustees to comply with its requirements. Breaches of confidentiality are treated seriously and may result in the individual concerned being required to leave the Trust.

1c Staff (including volunteers and consultants)

The information collected on staff is detailed in schedule 3. Staff are made aware at induction that a record is held about them and that they have the right to request access to it, and that the file may be sampled by the Trustees for quality checking purposes.

Purpose of collecting data

Basic data on employees, volunteers and consultants is collected upon recruitment for administration purposes.

Information sharing

Confidential information on staff, volunteers and consultants may be shared with the executive committee of trustees and reported to the whole Board anonymously if necessary.

The Trust will provide the Information Management Policy and procedure to all new staff, consultants and volunteers as a key part of their induction. All must comply with its requirements. Any failure to do so is gross misconduct and may result in a termination of their services.

2. BREACHES OF DATA PROTECTION

A breach of personal data is a security incident that has affected the confidentiality, integrity or availability of personal data.

If a breach occurs, the Trust will establish the likelihood of risk to an individual's rights and freedoms. If it is assessed that there is a risk, the Information Commissioner's Office (ICO) will be informed of any breach within 72 hours, even if not all details are yet available.

Existence of data subject's rights

The Trust informs all data subjects that they have rights pertaining to their data protection. Those rights are listed on page one in the section 'an individual's rights'.

In the case that a service user requests access to data held on them, the Trust will provide a copy of that information within one month of receiving the request in accordance with the GDRP stipulations.

In the case that a service user withdraws consent to have their information stored, the Trust will delete the individual's files from the database and destroy hard copies of information held on the individual.

RECORD KEEPING POLICY

Records are retained for the period specified in schedule 1 and, except for items that must be stored permanently, are then securely destroyed.

3. STORAGE PROCEDURES

- All paper records relating to service users, staff (including volunteers and consultants) and Trustees are kept in a locked filing cabinet.
- The web-based database containing confidential service user information is encrypted, password protected and regularly backed up. See Schedule 1 for more information.
- Confidential electronic files are kept securely on a cloud-based secure data centre, password protected and regularly backed up.
- The Trust complies with statutory requirements and records are maintained and retained in accordance with the retention summary in Schedule 1.
- The Trust complies with the Charities Statement of Recommended Practice in relation to its financial record keeping and reporting; and all financial records are retained in accordance with the retention summary in Schedule 1.
- The Trust stores insurance policies and employer's liability insurance certificates securely and in line with the retention summary in Schedule 1.

4. MOVING OR SENDING SENSITIVE INFORMATION

a) When sharing information outside the Trust by means other than face to face contact, the Trust follows the Trust's guidance within the Data Protection Policy, (see Schedule 3 attached).

b) The Trust risk assesses all means of sharing or carrying sensitive data about a family, staff member (including volunteers and consultants) or Trustee outside the office to ensure it is done so as securely as possible.
c) If sending information by post the Trust takes all steps necessary to ensure the recipient's details are accurate and that only the named person has access to the information.
d) When sending information by fax the Trust ensures the recipient is at hand when the fax arrives at its destination.
e) When sending information via email or a web portal the Trust ensures there is robust password protected access control in place and that only the intended recipient has access to it.
f) When storing or moving information via a mobile storage device e.g. laptop, tablet PC or memory stick, the Trust only does so if there are no safer alternative methods and only after a proper assessment of the risks attached thereto.

Responsible Trustee: Professor Ted Melhuish

Second Named Trustee: Simon Fuller

SCHEDULE 1 – RECORD RETENTION

Record Retention Periods for the Foundation Years Trust	
Employment In general, the personnel file should be retained for **6 years**, but need only contain sufficient information in to provide a reference. Copies of any reference given should be retained for 6 years after the reference request.	
Application form	Duration of employment, shred when employment ends
References received	May destroy 1 year after received, otherwise shred at end of employment
Sickness records	3 years (i.e. at end of employment, previous 3 year's records will be in the file, assuming employed for at least that period)
Annual leave records	2 years
Unpaid leave/special leave records	3 years
Records relating to injury or accident at work	12 years
References given/information to enable reference to be provided (including sickness)	6 years from end of employment
Recruitment and selection material	6 months after decision
Disciplinary records	6 years after employment ends
Disclosure and Barring Records	Certificate not kept by Trust. Note made of reference number, date of check & if satisfactory (or otherwise).
Trustee Records	
Basic Information	6 years after Trustee resigns from this role
Note: if an allegation has been made about a member of staff or Trustee, the record should be retained until they reach the normal retirement age or for 10 years, whichever is the later date.	
Family and volunteer records for the Foundation Years Trust	
Family records	File is retained for 7 years from the registration date. Files may be kept longer in the case of on-going child safety or welfare proceedings (10 years from date of any concern).
Volunteer files	File is retained for 12 months after the volunteer has ceased to volunteer. Sufficient information to provide a reference may be retained. For parents who join as volunteers, their files are kept in accordance with family records above.
Note: if an allegation has been made about the volunteer, the volunteer file should be retained until the volunteer reaches normal retirement age or for 10 years whichever is the later date.	
Financial Records	
Financial records	6 years
Payroll and tax information	6 years
Corporate	
Employer's Liability Certificate	40 years
Insurance policies	Permanently
Certificate of Incorporation	Permanently
Minutes of Board of Trustees	10 years from date of meeting
Memorandum & Articles of Association	Original to be kept permanently
Articles of Association	Original to be kept permanently
Variations to the Governing Documents	Original to be kept permanently
Membership records	20 years from commencement of membership register
Rental or Hire Purchase Agreements	6 years after expiry
Others	
Leases	12 years after lease has expired

SCHEDULE 2: THE SIX PRIVACY PRINCIPLES

1. Lawfulness, fairness and transparency

Transparency: Tell the subject what data processing will be done. Fair: What is processed must match up with how it has been described. Lawful: Processing must meet the tests described in GDPR [article 5, clause 1(a)].

2. Purpose limitations

Personal data can only be obtained for "specified, explicit and legitimate purposes" [article 5, clause 1(b)]. Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.

3. Data minimisation

Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" [article 5, clause 1(c)]. In other words, no more than the minimum amount of data should be kept for specific processing.

4. Accuracy

Data must be "accurate and where necessary kept up to date" [article 5, clause 1(d)]. Baselining ensures good protection and protection against identity theft. Data holders should build rectification processes into data management / archiving activities for subject data.

5. Storage limitations

Regulator expects personal data is "kept in a form which permits identification of data subjects for no longer than necessary" [article 5, clause 1(e)]. In summary, data no longer required should be removed.

6. Integrity and confidentiality

Requires processors to handle data "in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage" [article 5, clause 1(f)].

SCHEDULE 3 – RECORD OF DATA PROCESSING

Purpose of processing	Category	Category of personal data	Personal data	Source of data	Who shared with & how	How Stored
Staff administration	Employees	Personal Information	Name, address, home & mobile telephone numbers	Induction	Payroll company with password protected email	Locked cupboard/ secure cloud-based data centre
		Emergency contact info	Name of next of kin & contact telephone number	"	Not shared – internal use	As above
		Financial details	Bank account information, national insurance number and date of birth	"	Payroll company with password protected email	As above
Management of groups and events	Families	Personal information	i. Names, address, dates of birth of parents & children under 5 with home/mobile telephone numbers/ email (with consent to use) ii. SEN status and disabilities iii. Employment status, access to state benefits iv. Whether any children in family are subject to a child protection plan or other Children's Services plan v. Housing status vi. Benefits which apply to household vii. Access to a car in household viii. Allergies or health conditions	Registration & Data Form	With consent, with Children's Centre via gsx secure email	Secure web-based, encrypted database Paper copies in locked cabinet
		Special data	Ethnic origin	Registration & Data Form	As above	As above
		Consent	i. Permission to take photographs of parent and/or child(ren) ii. Signature to permit FYT to share this & other relevant info with partner agencies & use info for monitoring and evaluation purposes iii. Concerning virtual groups, consent via email or Facebook messenger	Registration & Data Form	As above	As above

Date policy was last adopted: 18 July 2019 Date of last review: 13 Nov 2020

		Attendance	Date and venue of attendance, with name of parent/carer(s) and child(ren)	Group registers	Not shared	As above
To prove FYT's impact	Families	Outcomes	Parent reporting questionnaires	2-4yrs or 0-2yrs questionnaires	Not shared	As above
			Anonymous ad hoc feedback from parents on enjoyment/impact of our groups	Verbal or captured in writing	Not shared	Locked filing cabinet
		Consent	Signed as agreement to participate in project, allow FYT to ask them to complete questionnaires, allow FYT to access information on child from nursery or school For online groups, consent via email or Facebook Messenger	Research Project Participation form	With WBC to show consent	Locked filing cabinet Consent documented on secure web-based, encrypted database
Trustee administration	Trustees	Personal information	Name, address, day & evening telephone numbers & date of birth	Charity Commission declaration	Charity Commission on their website	Locked cupboard/ secure cloud-based data centre
			As above, plus occupation	Form AP01 Companies House	Companies House on their website	Locked filing cabinet
Volunteer Administration	Volunteers	Personal information	Name, date of birth, address, telephone, email, name of next of kin & emergency contact information Also asks if anything needed to help us support them in their role.	FYT Volunteer information form	Not shared	Locked filing cabinet Secure web-based, encrypted database
		Attendance information	Dates of events & training attended	Registers	Not shared	As above
Training administration and group delivery	Early Years practitioners	Personal information	Name, email address, job title & place of work	Joining instructions	For PEEP training, shared with Peeple, with consent	As above