Family Refugee Support Project (FRSP)
Privacy Notice

What Our Privacy Notice Covers

- What information we collect from you and our lawful bases
- Why we collect this information
- Who might we share your information with
- What do we do with your information
- How long do we keep hold of your information
- How you can access the information we hold about you
- This policy does not cover the practices of companies other than FRSP or people who are not employed or managed by FRSP.

What Information do we collect from you?

We process the personal data of individuals, which includes:

- Names
- Addresses
- Telephone numbers
- Email addresses
- Financial details
- Employment details and educational details
- family details

We also process sensitive personal data, or 'special categories' of data, which includes:

- physical or mental health details
- racial or ethnic origin
- country of origin
- religious or other beliefs
- sexual orientation
- offences (including alleged offences)
- criminal and legal proceedings, outcomes and sentences
- data relating to asylum applications

Why does FRSP need to collect and store personal data?

FRSP undertakes a number of activities including:

- Provision of counselling and support services
- Training and supervision
- Marketing and fundraising
- Monitoring, evaluation and audit of service provision
- Staff, trustee and volunteer recruitment

In order for us to undertake the above we need to collect personal data from you for either correspondence purposes or detailed service provision, depending on the service you are accessing.

We have reviewed the purposes of our processing activities, and selected the most appropriate lawful basis for each activity. We believe that in order to achieve our duties and charitable objectives we have a **legitimate interest** to process the data for its relevant purpose, and are satisfied that there is no other reasonable way to achieve that purpose.

The basis of our legitimate interest is:

- Our use of your personal information is necessary to carry out a contract or take steps to enter into a contract with you
- We need to process your personal information to comply with relevant legal or regulatory obligations, which may include submitting reports to agencies or government departments. All data is anonymised for the purpose of reporting.

Our aim is not to collect unnecessary data, or store it for longer that its purpose.

Who might we share your information with?

If we need to pass sensitive identifiable data on to any third parties we will only do so where there is a service need and once we have obtained your explicit consent. In certain circumstances we will share your information without prior consent if we are legally required to do so, those circumstances are as follows;

- We receive a subpoena, court order or other legal demand for your information.
- We believe it is necessary to share information in order to investigate, prevent or take action regarding illegal activities, suspected fraud, to safeguard yourself or others, or as otherwise required by law.

What do we do with your information?

- The information that we collect and store relating to you is primarily used to enable us to provide our services to you, but we may also use this information to help us to improve our services to you.
- We will use this information to enable us to offer you appropriate services, to keep you informed and to seek feedback to monitor and evaluate our services.

How long do we keep hold of your information?

Please see the table below for retention periods.

How you can access the information we hold about you?

- You can ask us in writing, verbally or via email. We will record your request to access your data, noting the date and time this was requested.
- We ask for 28 days to provide access to your data. We might need to remove information from data files relating to your family members before we can share files, unless we have their permission to disclose this to you.

How we keep your personal information safe

We take appropriate measures to secure your personal information and protect it against unauthorised or unlawful processing, as well as against its accidental loss, destruction or damage, including:

- Using secure servers to store your personal information
- Using Secure Sockets Layer (SSL) software or other similar encryption technologies to encrypt confidential data in transit and at rest verifying the identity of individuals that access your personal information providing access to the minimum personal data necessary, using appropriate restrictions and making the data anonymous or unidentifiable whenever possible
- Using secured storage to store your personal information in media other than electronic

How you can contact us

If you have any question or concern on how we collect, handle, store or secure your personal information, contact our Data Protection Officer at:

Data Protection Officer
FRSP
Toxteth Town Hall
15 High Park Street
Liverpool
L8 8DX

Telephone: 0151 728 9340

info@frsp.org.uk

You also have the right to lodge a complaint with the Information Commissioner's Office (ICO):

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 0303 123 1113

Retention Periods

Record	**Retention Period**
Service User records including counselling and therapy notes.	7 years after closure of case or death to cover the time limit for any civil legal actions including contractual claims, unless otherwise requested by a service user or next of kin.
Staff employment records	6 years after employment ceases to cover the time limit for any civil legal actions including contractual claims
Application forms/interview notes for unsuccessful candidates	1 year
Trustee and Volunteer records	6 years after involvement with FRSP ends to cover the time limit for any civil legal actions including contractual claims
Financial records	7 years after a project ends to cover the time limit for any civil legal actions including contractual claims, unless otherwise specified by a funder.
Disclosure & Barring Service (DBS) Disclosures	No more than 6 months, unless in very exceptional circumstances it is considered necessary to keep certificate information for longer. In these cases, FRSP will consult with the Disclosure & Barring Service and will give full consideration to the Data Protection and Human Rights of the individual before doing so.
Minutes of Trustee meetings and Annual General Meetings; Annual Reports; FRSP publicity and information materials; Any other non-confidential FRSP documents.	Permanently