Background

This non-contractual privacy notice covers how we, St Francis' Children's Society, 'the data controller' collect, use, store and protect the data that is supplied to us by job applicants and agencies.

Data protection principles

The data protection principles which we will apply when gathering and using personal information are that:

1. we will process personal information lawfully, fairly and in a transparent manner;
2. we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;
3. we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;
4. we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;
5. we will keep personal information for no longer than is necessary for the purposes for which the information is processed; and
6. we will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

Our Commitment to Job applicants

We believe completely in equal opportunities and will treat all applicants fairly with no discrimination.

We never knowingly provide misleading information about the nature of the role. We would never charge a job seeker a fee for the purpose of finding them a role.

We are committed to managing your personal information securely and with respect in accordance with the General Data Protection requirements.

The information we collect may cover the following:

- Contact information (name address, phone number and email address)
- Information from the application form or covering letter (education, skills and qualifications)
- Health records & Health questionnaires where required as part of the role.
- Disclosure and Barring Record
- References from the named referees that the applicant provides and only with the applicants' consent.
- Visa and proof of the right to work in the UK documents
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Salary, annual leave, pension and benefits information.

We may also collect, store and use "special categories" of more sensitive personal data which require a higher level of protection such as Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions. Also information about criminal convictions and offences.

Purpose of collection

The purpose of collecting this information is to find suitable candidates to fulfil a specific role within the Society, and to check that you are legally entitled to legally work in the UK. We collect personal information either directly from candidates or sometimes from an employment agency. We may sometimes collect additional information background check agencies.

We will collect information about criminal convictions as part of the recruitment process. We are allowed to use your personal information in this way to carry out our obligations for an enhanced Disclosure and Barring Service certificate, in accordance with our Safeguarding Policy.

How the information is held.

Personal information may be held on Society premises and third party agencies, service providers, representatives and agents as described above and in cloud based IT services within the EU. Most information is transmitted by secure email (Egress) and is stored on our computers, paper based filing or retained on a cloud based file storage system which covers our email servers.

Our computers are safeguarded by anti-virus software and the regular changing of security passwords.

We keep the personal information that we obtain about you during the recruitment process for no longer than is necessary. How long we keep your personal information will depend on whether your application is successful, and you become employed by us, the nature of the personal information concerned and the purposes for which it is processed.

If your application is successful, we will keep only the recruitment personal information that is necessary in relation to your employment.

DBS Checks

All those who work on behalf of the Society in a paid or voluntary capacity will be subject to a DBS check at the appropriate level. This will be undertaken by the Senior Business Support Assistant and monitored by the Registered Manager who will countersign the paper copy to be kept on the individuals HR File.

The DBS Disclosure should be compared against the Self-Disclosure to highlight any issues for follow up. A Risk Assessment form will be completed if the DBS is not clear. This will be completed by the Registered Manager or Responsible Individual and a decision will then be taken.

Overseas checks will be taken up as required.

General principles

As an organisation using the Disclosure and Barring Service (DBS) checking service to help assess the suitability of applicants for positions of trust, St Francis' Children's Society complies fully with the code of practice regarding the correct handling, use, storage, retention and disposal of certificates and certificate information.

It also complies fully with its obligations under the General Data Protection Regulation (GDPR), Data Protection Act 2018 and other relevant legislation pertaining to the safe handling, use, storage, retention and disposal of certificate information.

Storage and access

Certificate information is kept securely, in lockable, non-portable, storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties.

The information is also stored on a secure electronic cloud based system within the EU.

Handling

In accordance with section 124 of the Police Act 1997, certificate information is only passed to those who are authorised to receive it in the course of their duties. We maintain a record of all those to whom certificates or certificate information has been revealed and it is a criminal offence to pass this information to anyone who is not entitled to receive it.

As an organisation registered with and inspected by Ofsted St Francis' Children's Society is legally entitled to retain certificate information for the purposes of inspection. This is to demonstrate 'safer recruitment' practice for the purpose of safeguarding audits. This practice is compliant with the Data Protection Act, Human Rights Act, General Data Protection Regulation (GDPR) and Adoption legislation, regulations and Adoption National Minimum standard 21.

Usage

Certificate information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

Retention

Once a recruitment (or other relevant) decision has been made, we do not keep certificate information for any longer than is necessary. This retention will allow for the consideration and resolution of any disputes or complaints, or be for the purpose of completing safeguarding audits.

Throughout this time, the usual conditions regarding the safe storage and strictly controlled access will prevail.

Disposal

Once the retention period has elapsed, we will ensure that any DBS certificate information is immediately destroyed by secure means, for example by shredding, pulping or burning. While awaiting destruction, certificate information will not be kept in any insecure receptacle (e.g. waste bin or confidential waste sack).

We will not keep any photocopy or other image of the certificate or any copy or representation of the contents of a certificate. However, not withstanding the above, we may keep a record of the date of issue of a certificate, the name of the subject, the type of certificate, the unique reference number of the certificates and the details of the recruitment decision taken.

Keeping your personal information secure

We have appropriate security measures in place to prevent personal information from being accidentally lost, or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it. Those processing personal information will do so only in an authorised manner and are subject to a duty of confidentiality. We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

Disclosure

We may disclose the information for the purpose of obtaining referees. Where additional information is required the information may be disclosed to the Disclosure and Barring Service, your G.P or an Occupational Health professional only after you have given your consent

You have specific rights in connection with personal information:

- **request access** to your personal information;
- **request correction** of the personal information that we hold about you;
- **request erasure** of your personal information;
    - ***In some circumstances, due to Adoption Legislation, you do not have the right to erase information***
- **object to processing** of your personal information where we are relying on a legitimate interest;
- **request the restriction of processing** of your personal information;
- **request the transfer** of your personal information to another party and the **right to withdraw consent.**

Your rights to correct and access your personal information and to ask for it to be erased

Please contact our Data Protection Contact (the Agency CEO), if (in accordance with applicable law) you would like to correct or request access to personal information that we

hold or if you have any questions about this notice. You also have the right to ask our Data Protection Contact for some, but not all, of the personal information we hold and process to be erased (the 'right to be forgotten') in certain circumstances.

Complaints

Privacy complaints are taken very seriously and if you believe that we have breached your privacy you should in the first instance write to the CEO stating the details of your complaint. We would ask that you provide us with as much detail as possible to allow a thorough investigation.

Should your complaint show that we have breached our duty of care we will report the breach to the Information Commissioner's Office

If you are not satisfied by our response you may complain to the ICO.