****

**General Data Protection Regulation (GDPR)**

**Privacy Notice**

We issue this privacy notice in the interests of transparency over how we use the personaldata that we collect from Job Applicants, Employees and Partners.

**What information does ISGBI collect?**

We collect and use a range of information about you. This includes as appropriate:

* name, address and contact details, including email address and telephone number;
* the terms and conditions of your employment;
* qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation;
* remuneration, including entitlement to benefits such as pensions and/or insurance cover;
* bank account and national insurance number;
* date of birth, gender and marital status;
* next of kin, dependants and emergency contacts;
* nationality and entitlement to work in the UK;
* periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
* any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
* assessments of your performance, including appraisals, performance reviews and ratings, performance improvement plans and related correspondence;  personal photographs

In addition to the above, ISGBI may also hold sensitive personal data consisting of information as to:

1. religious beliefs,
2. medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments;
3. the commission or alleged commission by you of any offence, any proceedings for any offence committed or alleged to have been committed by you, the disposal of such proceedings or the sentence of any court in such proceedings,
4. genetic data; and
5. biometric data where processed to uniquely identify a person (for example a photo in an electronic passport)

We may collect this information in a variety of ways. For example, data might be collected through:

* + application forms, CVs or resumes;
	+ passport or other identity documents such as your driving licence;
	+ forms completed by you at the start of or during employment (such as benefit nomination forms);
	+ correspondence with you; or
	+ interviews, meetings or other assessments.

In some cases, we may collect personal data about you from third parties, such as:

* + references supplied by former employers and others  information from criminal records checks permitted by law.

**Who is responsible for controlling the data?**

Fordata protection purposes the“**data controller**” means the person or organisation who determines the purposes for which and the manner in which any personal data are processed.

The data controller is The International Service Fellowship Trust, known as Interserve. Contact details are as follows:

Legal Entity: The International Service Fellowship Trust

Registered Address: Interserve, PO Box 17750, Birmingham, B9 9NU

Telephone No.: 03333 601 600

Charity Registration: 1020758

Company Registration: 02789773

OurData Protection Officer can be contacted at the address above, or by email at dataprotectionofficer@isgbi.org

**Why does the organisation process personal data?**

It is necessary for us to process personal data of Job Applicants, Employees and Partners for the following reasons:

1. To identify an individual for the purposes of recruitment;
2. To maintain the information for the general purposes of the ongoing employment relationship including performing the employment contract and maintaining the health and safety of individuals on our premises.

Our legal basis for processing personal data of applicants and staff is that:

1. Processing the personal data is necessary for the purpose of carrying out the employment contract or to take steps to enter into an employment contract;
2. Processing is necessary to comply with a legal obligation (for example we are obliged under employment law to include in a written statement of employment terms the identity of the parties to the employment contract); and/or
3. Processing the data is necessary for the purposes of our “**legitimate interests**” as the data controller (except where such interests are overridden by the interests, rights or freedoms of the individual).

Our “legitimate interests” for these purposes are:

1. the need to process data on applicants and staff for the purposes of assessing suitability for employment and then carrying out the employment contract;
2. the need to gather data for the purposes of safeguarding the health and safety of job applicants and employees;
3. the need to transfer employee data within the ISGBI Fellowship for administrative purposes; and
4. the need to process employee data for the purposes of ensuring network and information security.

We may from time to time need to process sensitive personal data, for example medical records or other information relating to the health and well being of an individual.

In that case we will either obtain the explicit consent of the individual to the processing of such data or we may consider the processing of that data as being necessary for carrying out our obligations as an employer. That will be assessed on a case by case basis.

There is no strict statutory or contractual requirement for you to provide data to us but if you do not provide at least that data that is necessary for us to assess suitability for employment and then to conduct the employment relationship then it will not practically be possible for us to employ you.

**Who has access to personal data?**

Your personal data may be received by the following categories of people:

1. Our People Care, Finance and communication Teams, as appropriate;
2. In the case of job applicants, the interviewer(s) and prospective manager;
3. Any individual authorised by us to maintain personnel files;
4. In the case of Partners, the relevant Country Team personnel and the relevant personnel within the receiving organisation;
5. Our professional advisers;
6. Appropriate external regulators and authorities (such as HMRC and HSE);
7. The International Office; and
8. Supporters who subscribe to prayer and news publications.

In some cases, the categories listed above will involve the need to transfer your data to a third country.  If we do this, we have procedures in place to ensure your data is sent using encryption and is password protected. Any transfer of your personal data will follow applicable laws and we will treat the information under the guiding principles of this Privacy Notice.

**How is the data stored?**

Data will be stored in a range of different places, including in your personnel file (both electronic and paper), in the organisation's HR management systems and in other IT systems (including the organisation's email system).

**How long does the organisation keep personal data?**

We will keep personal data for no longer than is strictly necessary, having regard to the original purpose for which the data was processed. Some data, such as account details for example, will be discarded shortly after the end of the employment contract.

In some cases we will be legally obliged to keep your data for a set period. Examples are below:

* Income tax and NI returns, income tax records and correspondence with HMRC: we are obliged to keep these records for a minimum of 3 years after the end of the financial year to which they relate.
* Wage and salary records: we are obliged to keep these records for 6 years.
* To comply with our safeguarding obligations we are obliged to maintain the following categories of data: name, dates of employment, role title, country and location of assignment, date and reference number of DBS check, dates and details

of child protection training undertaken; for 40 years after the end of your engagement with us.

**What are your rights in relation to your personal data?**

1. The right to be forgotten

You have the right to request that your personal data is deleted if:

1. it is no longer necessary for us to store that data having regard to the purposes for which it was originally collected; or
2. in circumstances where we rely solely on your consent to process the data (and have no other legal basis for processing the data), you withdraw your consent to the data being processed; or
3. you object to the processing of the data for good reasons which are not overridden by another compelling reason for us to retain the data; or
4. the data was unlawfully processed; or
5. the data needs to be deleted to comply with a legal obligation.

However, we can refuse to comply with a request to delete your personal data where we process that data:

1. to exercise the right of freedom of expression and information;
2. to comply with a legal obligation or the performance of a public interest task or exercise of official authority;
3. for public health purposes in the public interest;
4. for archiving purposes in the public interest, scientific research, historical research or statistical purposes; or
5. the exercise or defence of legal claims.

2. The right to data portability

You have the right to receive the personal data which you have provided to us, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided (us) where:

1. the processing is based on consent or on a contract; and
2. the processing is carried out by automated means.

Note that this right only applies if the processing is carried out by “automated means” which means it will not apply to most paper based data.

1. The right to withdraw consent

Where we process your personal data in reliance on your consent to that processing, you have the right to withdraw that consent at any time. You may do this in writing to the People Care team.

1. The right to object to processing

Where we process your personal data for the performance of a legal task or in view of our legitimate interestsyou have the right to object on “grounds relating to your particular situation”. If you wish to object to the processing of your personal data you should do so in writing to the People Care team stating the reasons for your objection.

Where you exercise your right to object we must stop processing the personal data unless:

* + we can demonstrate compelling legitimate grounds for the processing, which override your interests, rights and freedoms; or
	+ the processing is for the establishment, exercise or defence of legal claims. 5. The right of subject access

So that you are aware of the personal data we hold on you, you have the right to request access to that data. This is sometimes referred to as making a “subject access request”. For further details please refer to the Data Protection Policy.

1. The right to rectification

If any of the personal data we hold on you is inaccurate or incomplete, you have the right to have any errors rectified.

Where we do not take action in response to a request for rectification you have the right to complain about that to the Information Commissioner’s Office (ICO).

1. The right to restrict processing

In certain prescribed circumstances, such as where you have contested the accuracy of the personal data we hold on you, you have the right to block or suppress the further processing of your personal data.

1. Rights related to automated decision making and profiling

The GDPR defines “profiling” as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict:

* + performance at work;
	+ economic situation;
	+ health;
	+ personal preferences;
	+ reliability;
	+ behaviour;
	+ location; or
	+ movement

You have the right not to be subject to a decision when it is based on automated processing; and it produces a legal effect or a similarly significant effect on you.

However, that right does not apply where the decision is necessary for purposes of the performance of a contract between you and us. We may use data related to your performance or attendance record to make a decision as to whether to take disciplinary action. We consider that to be necessary for the purposes of conducting the employment contract. In any event that is unlikely to be an automated decision in that action will not normally be taken without an appropriate manager discussing the matter with you first and then deciding whether the data reveals information such that formal action needs to be taken. In other words there will be “human intervention” for the purposes of the GDPR and you will have the chance to express your point of view, have the decision explained to you and an opportunity to challenge it.

**Complaints**

Where you take the view that your personal data are processed in a way that does not comply with the GDPR, you have a specific right to lodge a complaint with the relevant supervisory authority. The supervisory authority will then inform you of the progress and outcome of your complaint. The supervisory authority in the UK is the ICO. The ICO contact details can be found at: <https://ico.org.uk/for-the-public/>.

I have received, read and agree to Interserve’s General Data Protection Regulations (GDPR) Policy and GDPR Privacy Notice.

…............................................................... ……………………………………

Name    Date

Please sign and return as part of your application