



## Future Frontiers Employee Privacy Notice

Future Frontiers (charity number: 1162470) (“**Future Frontiers**” or “**We**”) operates in the United Kingdom (“**UK**”). The UK has laws related to the collection, use, transfer and disclosure of the personal data of individuals, including employees and applicants. We take these obligations very seriously and are committed to protecting the privacy of our current and former employees and applicants.

The purpose of this Employee Privacy Notice (“**Privacy Notice**”) is to give employees who are based in the UK (“**Employees**”) and Future Frontier job applicants (“**Applicants**”) information about what personal data we collect, how we collect, use and disclose that data and the legal grounds for us doing this, and their rights in respect of their personal data. This Privacy Notice does not form part of your contract of employment and may be updated at any time.

For the purposes of the so-called “**UK GDPR**”, the “**controller**” of your personal data is Future Frontiers.

### 1. What Information We Collect About Employees and Applicants

Before, during and after their employment with the Future Frontiers, we may collect and process information about Employees and their spouse, domestic/civil partner or dependants (“**Dependants**”). We refer to such information in this Privacy Notice as “**Personal Data**”. Depending on whether you are an Employee or an Applicant, we collect the following Personal Data:

- **Personal Details:** Name, title, gender, date of birth, national insurance number, home contact details (email address, phone numbers, physical address), disability status, Free School Meal eligibility status;
- **Employment and compensation information:** Start date, length of service, job title, department, whether part-time or full-time, current salary, banking details, new starter forms, contract information and P45s;
- **Sensitive information:** Medical information and information relating to allergies (including dietary requirements); personal data revealing racial or ethnic origin; Disclosure and Barring Service (“**DBS**”) check information; and
- **Talent Management Information:** Details contained in letters of application and resume/CV (e.g., previous employment background, education history, professional qualifications and memberships, language and other relevant skills, certification, certification expiration dates), information necessary to complete a DBS check, information relating to references such as referees’ names and contact details;

If you are an Applicant and you provide us with the personal data of a referee as part of your application, it is your responsibility to obtain consent from that individual prior to providing the information to us.

## 2. Sources of Personal Data

If you are an Employee, we collect Personal Data from the following sources:

- **Employees and their Dependants:** In person, online (including message, files, data, documents, social media post or instant message communications), by telephone, or in written correspondence and forms, including any types of information transmitted to or from, received or printed from, or created, stored or recorded on our IT and communications.

If you are an Applicant, we collect Personal Data from the following sources:

- **Applicants:** in person, online, by telephone, or in written correspondence and forms;
- **Previous employers and other referees:** in the form of employment references;
- **Background check vendors (e.g. a DBS check):** as part of the recruitment process; and
- **Employment agencies and recruiters.**

## 3. How we use and disclose Personal Data

### Legal Basis for Processing

We will only use Personal Data when the law allows us to. Most commonly, we will use your Personal Data in the following circumstances:

- if you are an Employee, where it is necessary to perform obligations or exercise rights under your employment contract;
- if you are an Applicant, where it is necessary in order to take steps at your request prior to entering into an employment contract;
- where it is necessary to comply with a legal obligation (including, in respect of Sensitive Information, obligations under employment law) on us; and
- where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests. For example, the Future Frontiers has a legitimate interest in the processing of Personal Data for the centralisation of data processing activities, to design efficient and workable organisational processes, to allow organisational teams to work together and to make organisational processes more efficient and cost effective.

We may also use your Personal Data in the following situations, which are likely to be rare:

- where it is necessary to protect your (or someone else's) vital interests (and, in the case of Sensitive Information, where you are incapable of consenting);
- where it is necessary for us to defend, prosecute or make a claim against you, us or a third party; and
- in the case of Sensitive Information, where you have made the information public.

In particular, we may use your Sensitive Information, such as health/medical information, in order to accommodate a disability or illness, to reduce the risk of infectious diseases and to provide benefits. We may use your diversity-related Personal Data (such as race or ethnicity) in order to comply with legal obligations relating to diversity and anti-discrimination and/or measure and monitor diversity within Future Frontiers, and your criminal conviction data only where it is appropriate (given your role or the role for which you are applying) and we are legally able to do so.

#### Purposes of Processing

If you are an Employee, we process Personal Data for the following purposes:

- **Managing Workforce:** Managing work activities and personnel generally, including appraisals, performance management, promotions and succession planning, rehiring, administering salary, and payment administration and reviews, wages, healthcare, pensions and savings plans, training, leave, managing sickness leave, promotions, transfers, secondments, honouring other contractual benefits, providing employment references, performing workforce analysis and planning, performing employee surveys, performing background checks, managing disciplinary matters, grievances and terminations, reviewing employment decisions, making travel and off-site arrangements, managing expenses and reimbursements, planning and monitoring of training requirements and career development activities and skills, and creating and maintaining one or more internal employee directories;
- **Diversity Monitoring:** Collecting diversity monitoring data to comply with legal obligations and monitor and promote equal opportunities;
- **Communications and Emergencies:** Facilitating communication with you, ensuring organisational continuity, providing references, protecting the health and safety of employees and others, safeguarding IT infrastructure, office equipment and other property, facilitating communication with your nominated contacts in an emergency;
- **Future Frontiers Operations:** Operating and managing the IT and communications systems, managing product and service development, improving services, managing charity assets, allocating charity assets and human resources, strategic planning, project management, organisational continuity, compilation of audit trails and other reporting

tools, maintaining records relating to organisational activities, budgeting, financial management, reporting, and communications;

- **Compliance:** Complying with legal and other requirements, such as income tax and national insurance deductions, record-keeping and reporting obligations, conducting audits, compliance with government inspections and other requests from government or other public authorities, responding to legal process, pursuing legal rights and remedies, defending litigation and managing any internal complaints or claims, conducting investigations and complying with internal policies and procedures; and
- **Monitoring:** Monitoring our IT systems through manual and automated tools, and monitoring our physical premises and access to our physical premises. This is for general network operation and security, including the security of our IT systems and assets; for training employees; for the protection of confidential information; for investigating breaches of internal policies, fraud or other unlawful or wrongful activity; for organisational continuity (such as monitoring emails following an employee's departure); and for physical security of our premises.

If you are an Applicant, we process Personal Data for the following purposes:

- **Managing Workforce:** Managing recruitment and assessing your suitability, capabilities and qualifications for a job with us, processing your application and performing background checks if we offer you a job, such as DBS checks;
- **Communications:** Facilitating communication with you regarding your application;
- **Taking legal action:** Pursuing legal rights and remedies, defending litigation and managing any internal complaints or claims, conducting investigations and complying with internal policies and procedures; and
- **Compliance and safety:** Complying with legal (including, in respect of Sensitive Information, obligations under employment law) and other requirements, such as record-keeping and reporting obligations, conducting audits, compliance with government inspections.

We will only use your Personal Data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

#### Disclosures to third parties

We share Personal Data with the following unaffiliated third parties:

- **Service Providers:** Companies that provide products and services to the Future Frontiers such as third-party payroll service providers and pension providers; and

- **Public and Governmental Authorities:** Entities that regulate or have jurisdiction over the Future Frontiers such as regulatory authorities, public bodies, and judicial bodies, including to meet national security or law enforcement requirements.

#### 4. Transfer of Personal Data

Future Frontiers may disclose Personal Data throughout the world to fulfil the purposes described above. This may include transferring Personal Data to countries outside the UK that have different data protection regimes, and which are not deemed to provide an adequate level of protection for Personal Data. To ensure that Personal Data is sufficiently protected when transferred outside the UK, Future Frontiers has put in place protective measures. For further information regarding the Future Frontiers' protective measures, please contact us using the contact details in *Questions or Complaints*.

#### 5. Data Security

Future Frontiers will take appropriate measures to protect Personal Data that are consistent with applicable privacy and data security laws and regulations, including requiring service providers to use appropriate measures to protect the confidentiality and security of Personal Data.

#### 6. Data Retention

Future Frontiers' retention periods for Personal Data are based on organisational needs and legal requirements. We retain Personal Data for as long as is necessary for the processing purpose(s) for which the information was collected, as set out in this Privacy Notice, and any other permissible, related purposes.

#### 7. Your Rights

You have the right, in certain circumstances, to object to the processing of your Personal Data. You also have the right, in certain circumstances, to access your Personal Data, to correct inaccurate Personal Data, to have your Personal Data erased, to restrict the processing of your Personal Data, to receive the Personal Data you have provided to the Future Frontiers in a structured, commonly used and machine-readable format for onward transmission, and to object to automated decision-making.

Please note that certain Personal Data may be exempt from such access, correction, erasure, restriction and portability requests in accordance with applicable data protection laws or other laws and regulations.



You can also submit a complaint about our use of your Personal Data. To do so, you can contact the Information Commissioner's Office at: [www.ico.org.uk/make-a-complaint](http://www.ico.org.uk/make-a-complaint).

## 8. Questions or Complaints

Please contact us at [info@futurefrontiers.org.uk](mailto:info@futurefrontiers.org.uk) with any questions or complaints regarding this Privacy Notice or the Future Frontiers' privacy practices.