Recruitment Privacy Notice

Contents

1. Introduction

We are committed to protecting the privacy and respecting the rights of individuals with regard to the way in which we handle personal data. During the course of our recruitment activities we will process personal data about you. We recognise that the correct and lawful treatment of this personal data will maintain confidence, contribute to successful business operations and reduce the risk of privacy-related incidents arising.

2. The Information We Collect

- Your name, address and contact details, including email address and telephone number, date of birth and gender;
- The prospective terms and conditions of your employment;
- Details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the Group;
- Information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- Verbal Information about your nationality and entitlement to work in the UK;
- Information about your criminal record (role dependant);
- Details of your schedule (days of work and working hours) and attendance at work;
- Information on planned holiday;
- Information about medical or health conditions, including whether or not you have a disability for which we need to make reasonable adjustments;
- verbal information about whether you have been vaccinated which may be relevant for travel requirements and Covid-19 office guidelines;
- Camera images or video surveillance records (during visits to the ITF office for interviews); and
- Details of your bank account if we agree to reimburse your travel expenses for in-person interviews.

If we make an offer of employment, we will ask you for information so that we can carry out pre-employment checks. As part of the compliance screening checks you will be required to:

- Provide evidence of your Right to Work in the UK and national insurance number;
- Complete a Disclosure and Barring Service (DBS) check if applicable;
- Provide the name and the email address of two referees, one being your current or last employer; and
- Provide evidence of professional qualifications if applicable.

3. Where we Collect your Data From

Most of the personal data we hold about you is provided directly from you. For example, through the application and recruitment process, by completing forms and by corresponding with us by mail, phone, email.

We may also receive personal data about you from other sources such as:

- Employment / recruitment agencies;
- Previous employers or references;
- Background check providers (who in turn receive information public sources including the Disclosure and Barring Service, credit record agencies, education providers and previous employers).

We will also create personal data about you in the course of the recruitment process for example, interview notes.

4. Purpose and Legal Basis for Processing

Under data protection legislation we can only process your personal data if we have a legal basis listed within the GDPR or the DPA 2018 to do so. We will process personal data about you under the following legal bases:

- Processing is necessary in order to take steps to enter into a prospective employment contract with the ITF. For example, to assess your capability to perform the requirements of a role; to draft an employment contract; to contact references you have provided; to analyse CVs and interview notes; and to plan and organise your potential schedule of work, including travel requirements.
- Processing is necessary for compliance with a legal obligation to which we are subject. For example, to check your right to work in the UK, ascertain your fitness to work, and to prevent crimes such as fraud;
- Processing is necessary for the purposes of our (or a third party's) legitimate interests, except where such interests are overridden by your interests or fundamental rights and freedoms which require protection of personal data. Our legitimate interests include:
    - the running and management of our business, such as the planning and organisation of work, personnel management, IT Services, accounting and auditing;
    - to conduct data analytics studies to review and better understand employee retention and attrition rates;
    - the processing of personal data in connection with any actual or prospective litigation, internal or regulatory investigation.

We will only process your personal data for these specific purposes and legal bases, apart from in exceptional circumstances where we may rely on other legal bases permitted by law, such as where we consider that the processing is in your (or another's) vital interests. Your personal data will always only be processed to the extent that we consider that it is necessary for such purposes.

In addition, we require an additional justification in order to process personal data relating to criminal convictions and offences, and special categories of data (such as your medical information or your Covid-19 vaccination status). This will be either that:

- You have made such data publicly known in a clear and obvious way;
- It is necessary for the performance or exercise of obligations or rights which are imposed or conferred by law on us or you in connection with employment;
- It is necessary for reasons of substantial public interest, proportionate to the aim pursued, with respect for right to data protection and which provides measures to safeguard your rights;

- It is necessary to protect the vital interests of you or other employees and our stakeholders'/suppliers' personnel where you are legally incapable of giving consent;
- It is necessary for the purposes of occupational medicine or, for the assessment of your working capacity; and/or
- It is necessary for the establishment, exercise or defence of legal claims.

The main examples of how we will use your particularly sensitive personal information are:

- We will collect information about your criminal convictions history where we are entitled or required to carry out a criminal records check in order to satisfy ourselves that there is nothing in your criminal convictions history which makes you unsuitable for the role; and
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work; to prepare appropriate workplace adjustments; and to understand whether and subject to what conditions you are able to travel to perform your role.

5. Where You Are Required to Provide Personal Data

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during the recruitment process, for example contact details.

6. Automated Decision Making

We do not make decisions about you based solely on automated computer programs and all decisions taken in relation to you have some human intervention in the decisions taken.

7. Who We Share Your Personal Data With

Your personal data will be shared internally, including with members of the HR, Safeguarding and Recruitment teams, the recruiting line manager and other managers in that team/department, if access to the data is necessary for performance of their roles.

We also share your personal data with third parties for limited purposes, some of which may be located in other countries (where indicated) such as:

- Background Screening Service Providers – currently via First Advantage (UK and Overseas) which run appropriate background and criminal checks on prospective and current employees to ensure there have been no issues to flag;
- IT platforms including DocuSign and RefNow;
- Auditors and professional advisors, such as lawyers and consultants so that we can protect our legitimate business interests and comply with applicable laws and regulations;
- IT providers such as disaster recovery management systems, storage back-up providers for the ITF's critical servers, archive storage providers, cloud storage and file sharing websites, client relationship management systems, in order to protect our legitimate business interests and comply with applicable laws and regulations;
- Security solution providers which maintain our CCTV systems in order to protect our legitimate business interests; and

- If we are under a duty to disclose or share personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others.

8. Sharing your Personal Data Internationally

As a company operating globally, we would rarely be required to transfer and process your personal data worldwide. We do not share your application or associated information outside the EEA.

9. Protecting your Personal Data

The ITF takes the security of your personal data seriously. We have internal policies and controls in place to ensure that your personal data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the proper performance of their duties.

When we need to disclose your personal data to a supplier, business partner, or other third party, we will seek to ensure that they will provide appropriate technical and organisational security measures to safeguard your personal data. We will do this by entering into a contract or other arrangement with them and where necessary carrying out ongoing due diligence checks of their security measures.

10. Retention of your Personal Data

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

We will hold your personal data for the duration of the recruitment campaign. If your application is successful we will store the information securely for the length of your employment with the ITF. If your application is unsuccessful we will store the information securely for 6 months from the date we inform you of our decision.

11. Your Rights

You have the right to:

- Request information about whether we hold personal data about you and, if so, what that information is and why we are holding/using it.
- Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below).
- Object to processing of your personal data where we are relying on a legitimate interest (or that of a third party) and there is something about your particular situation which makes you want to object to processing on this ground.

- Request the restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data e.g. if you want us to establish its accuracy or the reason for processing it.
- Request transfer of personal data (that you have provided to us) in an electronic and structured form to you or to another party (commonly known as a "right to data portability"). This enables you to take your personal data from us in an electronically useable format and transfer it to another party.

If you want to exercise any of these rights, then please contact our Data Protection team in the first instance (dataprotectionofficer@itftennis.com).

You will not have to pay a fee to access your personal data (or to exercise any of the other above rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

12. Your Right to Complain

If you have a complaint about our use of your personal data, we would prefer you to raise this with us in the first instance to give us the opportunity to put it right.

Please contact our Data Protection team in the first instance (dataprotectionofficer@itftennis.com).

You can also contact the Information Commissioner's Office, via their website at www.ico.org.uk/concerns or write to them at:

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

13. Changes to this Privacy Notice

This Privacy Notice does not form part of your prospective contract of employment and may be amended by the ITF, in its absolute discretion, at any time. Any changes to it will be communicated to you by way of an email, social media or a notice on our website.

14. Further Information

If you have any questions, please contact the ITF Data Protection team (dataprotectionofficer@itftennis.com).

15. Appendix A- Definitions

The following definitions of terms used in this document are drawn from Article 4 of the GDPR:

- **Personal Data:** Any information relating to an identified or identifiable natural person ("**Data Subject**") who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more

factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- **Data Subject:** An identifiable natural person is one who can be identified, directly or indirectly
- **Controller**: The natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.
- **Processor**: A natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.
- **Processing**: An operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of the data.
- **Profiling:** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- **Special Category Data:** means the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
- **Third party:** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

