



Privacy Notice for Employees, Candidates and Supporters

The Recruitment Junction is committed to protecting the privacy and security of your personal data. This privacy notice details how The Recruitment Junction collects and uses personal data about you during and after your working relationship with us, in accordance with the UK General Data Protection Regulation (**UK GDPR**).

It applies to all employees of The Recruitment Junction, all candidates who engage the services of The Recruitment Junction and all supporters who support The Recruitment Junction (as either a donor or volunteer). Please read this privacy notice carefully before you provide us with any personal data so that you fully understand how your data is collected and used by The Recruitment Junction.

Important personal data and who we are

The Recruitment Junction is a "data controller". This means that we are responsible for deciding how we hold and use personal data about you. We are required under data protection legislation to notify you of the personal data contained in this privacy notice.

This notice applies to current and former employees, supporters and candidates. This notice does not form part of any contract to provide services between The Recruitment Junction and you. We may update this notice at any time but if we do so, we will provide you with an updated copy of this notice as soon as reasonably practical.

It is important that you read and retain this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal data about you, so that you are aware of how and why we are using such personal data and what your rights are under the data protection legislation.

Data protection principles

We will comply with data protection law. This says that the personal data we hold about you must be:

- used lawfully, fairly and in a transparent way;
- collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;
- relevant to the purposes we have told you about and limited only to those purposes;
- accurate and kept up to date;
- kept only as long as necessary for the purposes we have told you about; and
- kept securely.

The personal data we collect

Personal data means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

Depending on how you are involved with us, we will collect your personal data under one or more of the following legal bases:

- **consent** – we may be able to offer you a choice as to whether or not we collect, store, share or otherwise process your personal data. This will be made clear to you and will not be done unless we have your consent;
- **contract** – in some cases we need to collect personal data to fulfil a contract, this personal data will always be anonymised. For example, where we are required to report on candidate diversity;
- **legitimate interest** – where processing is necessary for the purposes of our legitimate interests, except where such interests are overridden by your interests or fundamental rights and freedoms which require protection of personal data;
- **legal obligation** – sometimes we may need to store and share personal data where we have a legal obligation to do so. For example, we may need to store personal data to comply with health and safety legislation; and/or
- **public interest** – where we are working to assist with public law we will collect your personal data under public interest. We will be clear about why we have to collect this personal data, how it will be used, who you can expect it to be shared with and why

To carry out our core activities, we collect, store and use personal data about you which may include:

- your name and title;
- address and postcode;
- date of birth;
- gender;
- marital status and dependants;
- private and corporate e-mail address;
- phone number;
- employment history;
- education history;
- financial personal data and compliance documentation;
- references verifying your qualifications and experience;
- documents that verify your right to work in the United Kingdom;
- curriculum vitae;
- photograph;
- employment details and preferences; and/or
- links to your professional profiles available in the public domain e.g. LinkedIn, Twitter, Facebook for Business or corporate website.

Some of the personal data we collect about you is considered as being sensitive personal data, which requires a higher level of protection. This may include:

- age;
- race or ethnicity;
- sexual preferences;
- alcohol and other drug use;
- trade union membership;
- disability or other illness, physical or mental health including any medical condition, health and sickness records, including:
 - records relating to your leaving employment for reason of ill-health, injury or disability; and
 - details of any absences (other than holidays) from work including time on statutory parental leave and sick leave;
- criminal convictions/offending behaviour;
- experience of homelessness;



- experience of the care system; and/or
- experience in the armed forces.

How we collect this personal data

We collect personal data about employees, supporters and candidates in the following ways:

- by corresponding with us by phone, e-mail or otherwise;
- by engaging with us to receive our services or act as a volunteer; and/or
- by attending our events.

We may also obtain personal data about you from other sources such as LinkedIn, Twitter, Facebook, corporate websites, job Board websites, online CV libraries, your business card, personal recommendations, and any relevant social media sites.

We may sometimes collect additional information from third parties including former employers or background check agencies.

How we use the personal data we collect about you

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

- where we need to perform the contract we have entered into with you;
- where we need to comply with a legal obligation; and/or
- where it is necessary for legitimate interests pursued by us or a third party and your interests and fundamental rights do not override those interests.

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

- where we need to protect your interests (or someone else's interests); or
- where it is needed in the public interest.

We need all the categories of information in section 0 above to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases, we may use your personal data to pursue our legitimate interests, except where such interests are overridden by your interests or fundamental rights and freedoms which require protection of personal data. Some of these grounds for processing will overlap and there may be several grounds which justify our use of your personal data.

The situations in which we will process your personal data are listed below:

- if you are a supporter, we will primarily use the personal data that you provide to us to contact you with personal data about our work and future fundraising events. If you are a supporter who is also a volunteer, we will primarily use the personal data that you provide to us to allow us to support and manage your volunteering role. However, we may also use your personal data to do the following:
 - maintaining records;
 - complying with health and safety obligations;
 - education, training and development requirements;
 - communicating about your volunteering role;
 - keeping you and others safe while volunteering;

- in risk assessments, to put in place countermeasures for identified risks; and
 - equal opportunities monitoring.
- if you are an employee, we will primarily use the personal data that you provide to us to allow us to perform our role as employer; to enable us to comply with legal obligations. However, we may also use your personal data to do the following:
 - making a decision about your recruitment or appointment;
 - determining the terms on which you work for us;
 - checking you are legally entitled to work in the UK;
 - paying you and, if you are an employee, deducting tax and National Insurance contributions;
 - liaising with your pension provider, providing information about changes to your employment such as promotions, changing in working hours;
 - general administration of the contract we have entered into with you;
 - business management and planning, including accounting and auditing;
 - conducting performance reviews, managing performance and determining performance requirements;
 - making decisions about salary reviews and compensation;
 - assessing qualifications for a particular job or task, including decisions about promotions;
 - gathering evidence and any other steps relating to possible grievance or disciplinary matters and associated hearings;
 - making decisions about your continued employment or engagement;
 - making arrangements for the termination of our working relationship;
 - education, training and development requirements;
 - dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work;
 - ascertaining your fitness to work, managing sickness absence;
 - complying with health and safety obligations;
 - to prevent fraud;
 - to monitor your business and personal use of our information and communication systems to ensure compliance with our IT policies;
 - to ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution;
 - to conduct data analytics studies to review and better understand employee retention and attrition rates;
 - equal opportunities monitoring;
 - dealing with Freedom of Information Act/Environmental Information Regulations requests, and
- if you are a candidate, we will primarily use the personal data that you provide to us to allow us to perform our contract with you to facilitate placing you with a partner organisation. However, we may also use your personal data to do the following:
 - making a decision about your engagement with a partner organisation;
 - checking you are legally entitled to work in the UK;
 - administering the contract for service that we have entered into with you;
 - assessing qualifications for a particular job or task with a partner organisation;
 - making decisions about your continued engagement with us;
 - making arrangements for the termination of our working relationship;
 - education, training and development requirements prior to your engagement with a partner organisation;
 - ascertaining your fitness to work with a partner organisation;
 - complying with our health and safety obligations; and
 - to prevent fraud.

If you fail to provide certain personal data when requested, we may not be able to perform the contract we have entered into with you, or we may be prevented from complying with our legal obligations.

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. If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

How we use particularly sensitive personal data we collect about you

"Special categories" of particularly sensitive personal data, such as information about disability or other illness, physical or mental health and criminal convictions/offending behaviour, require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal data in the following circumstances:

- in limited circumstances, with your explicit written consent;
- where we need to carry out our legal obligations or exercise rights in connection with employment;
- where it is needed in the public interest; and/or
- where it is necessary to protect you or another person from harm.

Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

In general, we will not process particularly sensitive personal data about you unless it is necessary for performing or exercising obligations or rights in connection with the contract between us. On rare occasions, there may be other reasons for processing, such as it is in the public interest to do so.

The situations in which we will process your particularly sensitive personal data are listed below:

- to assess a candidate's eligibility for our services;
- to assess a candidate's readiness for work and to inform a partner organisation about appropriate workplace adjustments;
- to determine a candidate's suitability for a vacancy we are working on. For example, when a partner organisation has taken the decision to take positive action and is seeking to address under-representation of a particular group of people with one or multiple protected characteristics such as disability or ethnicity in their workforce; and/or
- if we reasonably believe that you or another person are at risk of harm and the processing is necessary to protect you or them from physical, mental or emotional harm or to protect physical, mental or emotional well-being.

We do not need your consent if we use special categories of your personal data in accordance with our written policy to carry out our legal obligations or exercise specific legal rights.

In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

We do not need your consent where the purpose of the processing is to protect you or another person from harm or to protect your well-being and if we reasonably believe that you need care and support, are at risk of harm and are unable to protect yourself.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

We will hold personal data about criminal convictions, and we will process this information in the situations listed in section 6 above.

We are allowed to use your personal data in this way as part of performing or exercising obligations or rights in connection with the contract between us. We have in place an appropriate policy and safeguards which we are required by law to maintain when processing such data.

Disclosing the personal data which we collect

We will share your personal data with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

We may share the personal data that you provide to us with third parties in the following situations:

- with partner organisations, including referral partners, other specialist service providers and employers, to facilitate the provision of our recruitment consultancy services as well as pre-work and post-placement support services
- with the police or the local authorities where we consider this necessary to protect the safety of yourself or others

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal data in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

Your personal data is not disclosed to third parties for marketing or advertising purposes unless with your express and written consent.

We will not transfer your personal data outside the EU.

How we keep your personal data safe

We have put in place appropriate technical and organisational measures to protect the personal data you provide to us. Although we take appropriate measures to prevent personal data from being lost, destroyed, damaged or unlawfully processed, we cannot guarantee this will not occur. Further details of these measures may be obtained upon request.

To protect candidate's and employee's personal data, we use the following security measures:

- **recruiting software** – we use recruiting software to keep candidates' personal data private. Each user of our recruitment software has a certain level of access assessed as appropriate to facilitate their work. This access is reviewed regularly and provided following a thorough induction and the signing of the relevant policies. With recruiting software, we can store candidate and supporter personal data in one place for easy access and safekeeping.
- **strong passwords** – securing personal data begins with using strong passwords. The more complex the passwords are, the better. Instead of using the same password for everything or a variation of passwords, we use unique passwords with multiple numbers, symbols, and letters. These passwords are used to protect documents, such as candidate forms that include personal data. The password provides an extra layer of protection to secure candidate or employee personal data.
- **secure networks** – network security is crucial inside and outside the office. All of our employees make sure their system is secure when accessing candidate files or personal data by using a firewall, password protecting the network, and using a virtual private network (VPN) to keep data secure.
- **awareness** – cybersecurity is a top priority when handling sensitive candidate personal data. Hackers create new and innovative threats every day. If you receive an email asking you to click on a suspicious link or provide private personal data about a candidate, do not click on it. Report the threat to us as soon as possible and delete the email.

In addition, we limit access to your personal data to third parties who have a business need to know. They will only process your personal data on our instructions, are subject to a duty of confidentiality, and are also required to take appropriate measures to protect that personal data.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

How long we keep your personal data for

We retain different types of data for differing periods, but will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements

The criteria we use to determine whether we should retain your data and how long for includes:

- 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;
- any applicable legal requirements.
- the perceived accuracy of your data;
- your engagement levels with our services; and
- our legal obligations following a job offer or when a placement has been made.

We may archive part of or all your personal data or retain it on our financial systems but delete all or part of it from our recruitment software system. On removal, we may anonymise parts of your personal data – particularly following a request for suppression or deletion of your personal data – to ensure we do not re-enter your personal data to our database unless you have requested us to do so.

Our current retention period for personal data of candidates who have not been placed or are no longer showing any signs of engagement with us via any modes of contact including by phone and email is six years.

Your rights in connection with personal data

The GDPR provides you with the following rights:

- **to be informed** about the personal data we process about you;
- **to request access** to the personal data we process about you. This is commonly known as a "data subject access request" and enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it;
- **to request correction** of your personal data. This enables you to have any incomplete or inaccurate information we hold about you corrected;
- **to request erasure** of your personal data in certain circumstances, 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);
- **to request the restriction of processing.** This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it;
- **to request the transfer** of your personal data to another party;
- **to object to the processing** of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal data for direct marketing purposes
- **not to be subjected to automated decision-making and profiling.**

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your contractual relationship with us.

If you want to review, verify, correct or request erasure of your personal data, object to the processing of your personal data, or request that we transfer a copy of your personal data to another party, please contact Beverley Brooks in writing using the contact details at the end of this privacy notice.

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

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.



Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and any changes we make to our privacy notice will be posted on our website and, where appropriate, you will be notified by e-mail. Please check back frequently to view any updates or changes to our privacy notice.

Please send any questions, comments or requests relating to this privacy notice to beverley.brooks@therecruitmentjunction.com.

Date of issue: January 2021