



Applicant Privacy Notice

The Royal Osteoporosis Society is aware of its obligations under the General Data Protection Regulation (GDPR) and is committed to processing your data securely and transparently. This privacy notice sets out, in line with GDPR, the types of data that we collect and hold on you as a job applicant. It also sets out how we use that information, how long we keep it for and other relevant information about your data.

Data controller details

The Royal Osteoporosis Society is a data controller, meaning that it determines the processes to be used when using your personal data. Our contact details are as follows:

The Royal Osteoporosis Society
Camerton
Bath, BA2 0PJ

Data protection principles

In relation to your personal data, we will:

- process it fairly, lawfully and in a clear, transparent way
- collect your data only for reasons that we find proper for the course of your employment in ways that have been explained to you
- only use it in the way that we have told you about
- ensure it is correct and up to date
- keep your data for only as long as we need it
- process it in a way that ensures it will not be used for anything that you are not aware of or have consented to (as appropriate), lost or destroyed

Types of data we process

We may hold many types of data about you that you have provided as part of submitting an application, including:

- your personal details including your name, and email address
- whether or not you have a disability

How we collect your data

We collect data about you in a variety of ways including the information you would normally include in a CV or a job application cover letter, or notes made by our recruiting officers during a recruitment interview.

- information included on your CV including references, education history and employment history
- documentation relating to your right to work in the UK

Further information will be collected directly from you as part of our onboarding processes if you are successful in being offered a position, when you complete forms, for example, your bank and emergency contact details. Other details may be collected directly from you in the form of official documentation such as your driving licence, passport, relevant qualifications or other right to work evidence.

In some cases, we will collect data about you from third parties, such as employment agencies and former employers when gathering references.

Personal data is kept securely in personnel files or within the charity's HR and IT systems.

How we use your personal data

We use your personal data to:

- review and process your application
- to keep you up to date on its progress
- to resolve grievances and complaints that involve you
- in relation to any right to work information we collect, in order to ensure we comply with the law in employing you
- in relation to any criminal record checks we complete, in order to ensure we comply with charity policy

Why we process your data

The law on data protection allows us to process your data for certain reasons only:

- in order to perform the employment contract that we are party to
- in order to carry out legally required duties
- in order for us to carry out our legitimate interests
- to protect your interests and
- where something is done in the public interest.

All of the processing carried out by us falls into one of the permitted reasons. Generally, we will rely on the first three reasons set out above to process your data.

We need to collect your data to ensure we are complying with legal requirements such as:

- carrying out checks in relation to your right to work in the UK and
- making reasonable adjustments for disabled employees.

We also collect data so that we can carry out activities which are in the legitimate interests of the charity. We have set these out below:

- operating a fair and transparent recruitment process
- recruiting and retaining the right candidates
- ensuring candidates have the right skills and experience for any given role
- resolving any complaints in a fair and transparent manner
- making decisions about who to offer employment to
- making decisions about salary and other benefits
- assessing training needs
- dealing with legal claims made against us

If you are unsuccessful in obtaining employment, your data will not be used for any reason other than in the ways explaining in relation to the specific application you have made.

Special categories of data

Special categories of data are data relating to your:

- health
- sexual orientation
- race
- ethnic origin
- political opinion
- religion
- trade union membership and
- genetic and biometric data.

We must process special categories of data in accordance with more stringent guidelines. Most commonly, we will process special categories of data when the following applies:

- you have given explicit consent to the processing
- we must process the data in order to carry out our legal obligations
- we must process data for reasons of substantial public interest
- you have already made the data public.

We will use your special category data:

Health information

In terms of the health information collected:

- **If you are invited to an assessment;** we will ask if you require any special arrangements or adjustments to be made for your assessment. The provision of this information is likely to include special category (health) data and is therefore covered by data protection law. We ask for this information so that we are fully aware of any adjustments needed and we will use the information provided to inform our decisions about making those changes. We rely on our

legal obligation to meet the requirements of the Equality Act 2010 as the lawful basis for processing your data.

- **If you are successful in being offered a position;** we will ask you to complete a health questionnaire and there is a specific condition for processing this special category of data. Processing is necessary for the purposes of assessing the working capacity of the employee and ensuring reasonable adjustments are in place to support the employee in fulfilling their role.

All health information is securely held by the Human Resources Department and will only be shared with the recruiting manager or the employee's line manager where it is appropriate to do so.

Criminal conviction data

We will only collect criminal conviction data where it is appropriate given the nature of your role and where the law permits us. This data will be collected if you are successful in being offered a position and may also be collected during your employment. We use criminal conviction data in the following ways:

- to form part of an overall recruitment screening assessment, in line with safer recruitment practices.

This information is securely held by the Human Resources Department and will only be shared with the employee's line manager where it is appropriate to do so.

If you do not provide your data to us

One of the reasons for processing your data is to allow us to carry out an effective recruitment process. Whilst you are under no obligation to provide us with your data, we may not be able to process, or continue with (as appropriate), your application.

Sharing your data

Your data will be shared with colleagues within the charity where it is necessary for them to undertake their duties with regard to recruitment. This includes, for example, the HR department, those in the department where the vacancy is who are responsible for screening your application and interviewing you, the IT department where you require access to our systems to undertake any assessments requiring IT equipment.

In some cases, we will collect data about you from third parties, such as employment agencies.

Your data will be shared with third parties if you are successful in your job application. In these circumstances, we will share your data in order to obtain references as part of the recruitment process and if appropriate, obtain a criminal records check.

We do not share your data with bodies outside of the European Economic Area.

Protecting your data

We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such which are outlined in our Data Protection Policy found by logging onto www.theros.org.uk/yourdata

Where we share your data with third parties, we provide written instructions to them to ensure that your data are held securely and in line with GDPR requirements. Third parties must implement appropriate technical and organisational measures to ensure the security of your data.

How long we keep your data for

In line with data protection principles, we only keep your data for as long as we need it for, and this will depend on whether or not you are successful in obtaining employment with us.

If your application is not successful and we have not sought consent or you have not provided consent upon our request to keep your data for the purpose of future suitable job vacancies, we will keep your data for 6 months once the recruitment exercise ends.

If we have sought your consent to keep your data on file for future job vacancies, and you have provided consent, we will keep your data for 12 months once the recruitment exercise ends. At the end of this period, we will delete or destroy your data, unless you have already withdrawn your consent to our processing of your data in which case it will be deleted or destroyed upon your withdrawal of consent.

If your application is successful, your data will be kept and transferred to the systems we administer for employees. We have a separate privacy notice for employees, which will be provided to you.

Automated decision making

No decision will be made about you solely on the basis of automated decision making (where a decision is taken about you using an electronic system without human involvement) which has a significant impact on you.

Your rights in relation to your data

The law on data protection gives you certain rights in relation to the data we hold on you. These are:

- the right to be informed. This means that we must tell you how we use your data, and this is the purpose of this privacy notice
- the right of access. You have the right to access the data that we hold on you. To do so, you should make a subject access request
- the right for any inaccuracies to be corrected. If any data that we hold about you is incomplete or inaccurate, you are able to require us to correct it

- the right to have information deleted. If you would like us to stop processing your data, you have the right to ask us to delete it from our systems where you believe there is no reason for us to continue processing it
- the right to restrict the processing of the data. For example, if you believe the data we hold is incorrect, we will stop processing the data (whilst still holding it) until we have ensured that the data is correct
- the right to portability. You may transfer the data that we hold on you for your own purposes
- the right to object to the inclusion of any information. You have the right to object to the way we use your data where we are using it for our legitimate interests
- the right to regulate any automated decision-making and profiling of personal data. You have a right not to be subject to automated decision making in way that adversely affects your legal rights.

Where you have provided consent to our use of your data, you also have the unrestricted right to withdraw that consent at any time. Withdrawing your consent means that we will stop processing the data that you had previously given us consent to use. There will be no consequences for withdrawing your consent. However, in some cases, we may continue to use the data where so permitted by having a legitimate reason for doing so.

If you wish to exercise any of the rights explained above, please contact the HR Team, Royal Osteoporosis Society, Camerton, Bath BA2 0PJ or email recruitment@nos.org.uk.

Making a complaint

The supervisory authority in the UK for data protection matters is the Information Commissioner (ICO). If you think your data protection rights have been breached in any way by us, you are able to make a complaint to the ICO.

Data Protection Officer

The charity's Data Protection Officer is **Juliette Morgan, Head of Corporate Governance** and she can be contacted on juliette.morgan@theros.org.uk 01761 473251.