Employee Privacy Notice - *How we use your personal information*

Who we are

To operate as a housing business, RHP Group (the Group) must get, process and store personal data about our applicants for housing, tenants, and customers. This Privacy Notice supports our Data Protection Policies and it explains how the Group treats your personal data as an employee.

Our Privacy Promise

We promise:

- ✓ To keep your data safe and secure
- ✓ Treat any data concerns you may have as priority

Purpose of this notice

This privacy notice gives you information on how we collect and process your personal data throughout your working relationship with us. It makes you aware of how and why your personal data will be used, namely for the purposes of the performance of our contract with you as our employee, and how long it will usually be retained for. In these cases, we will be the "data controller" for the purposes of data protection laws.

This notice provides you with the information that must be provided under the UK General Data Protection Regulation (the UK GDPR), the Data Protection Act 2018 (DPA 2018) and any subsequent legislation. We will only process your personal data in accordance with this Privacy Notice unless otherwise required by applicable law. We take steps to ensure that the personal data that we collect about you is adequate, relevant, not excessive, and processed for limited purposes.

Who we share your personal data with

For the purposes of this Privacy Notice, personal data means any information about an identifiable individual. Personal data excludes anonymous or de-identified data that is not associated with a particular individual. To carry out our activities and obligations as an employer, we may collect, store, and process the following categories of personal data, which we require to administer the employment relationship with you:

- ✓ Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- ✓ Date of birth.
- ✓ Gender.
- ✓ Marital and dependent status, only when needed to administer benefits such as health insurance or pension benefits.
- ✓ Beneficiary and emergency contact information.
- ✓ Government identification numbers such as national insurance number, driver's license number, or other identification card number.
- ✓ Your contract of employment and any amendments to it.
- ✓ Bank account details and payroll information.
- ✓ Wage and benefit information.
- ✓ Compensation history.
- ✓ Appraisals, disciplinary and grievance history.
- ✓ History of holidays, sickness absence and other types of leave.

- ✓ Letters produced at your request like a letter to your mortgage company confirming your salary
- ✓ Performance information.
- ✓ Insurance enrolment information.
- ✓ Start date and job title.
- ✓ Location of employment.
- ✓ Education and training.
- ✓ Employment records (including professional memberships, references, work history, and proof of work eligibility).
- ✓ Photograph.
- ✓ Other personal details included in a CV, application form or cover letter or that you otherwise voluntarily provide to us.
- ✓ Information regarding your use of any company vehicles.
- ✓ Information regarding your use of any company computers, IT systems, mobile telephones and tablets and keep records of usage. This is detailed in our Information Security Policy and Mobile Device Policy which can be found on Lighthouse.
- ✓ Details of hour hours of work by way of our clocking on and off system (for those employees who use the Efficient Flexi time system).
- ✓ We also use CCTV throughout our premises and therefore you may appear on CCTV footage.

The personal data is mandatory in order for us to administer the employment relationship. Failure to provide or allow us to process mandatory personal data may affect our ability to accomplish the purposes stated in this Privacy Notice.

We will collect the majority of the personal data that we process directly from you. In limited circumstances third parties may provide your personal data to us, such as former employers, official bodies (such as regulators or the Disclosure and Barring Service), or medical professionals.

How your information will be used

As your employer, the Group needs to keep and process information about you for normal employment purposes. The personal data we hold, and process will be used for the management and administrative of your contract with us, during your employment. We will keep and use the information to enable us to run the business and manage our relationship with you effectively, lawfully, and appropriately. We do not use automated decision making or profiling.

The information you provide will be used whilst you are working for us and at the time when your employment ends and after you have left. We will only use your personal information when the law allows us to. Mostly commonly, we do this to enable us to comply with the employment contract and with any legal requirements, pursue the legitimate interests of the Group and protect to our legal position in the event of legal proceedings, or with your consent if applicable law requires consent. We may also use your information where we need to protect your vital interests or if it is the public interest to do so.

We may process your personal data for the following legitimate business purposes and for the purposes of performing the employment contract with you:

- ✓ Deciding about your appointment.
- ✓ Determining the terms on which you work for us.
- ✓ Checking you are legally entitled to work in the UK.

- ✓ Administering the contract, we have entered into with you.
- ✓ Employee administration (including payroll and benefits administration).
- ✓ Business management and planning.
- ✓ Processing employee work-related claims (for example, insurance and worker's compensation claims).
- ✓ Accounting and auditing.
- ✓ Making decisions about salary reviews.
- ✓ Managing any sickness absence and ascertaining fitness to work.
- ✓ Conducting performance reviews and determining performance requirements.
- ✓ Assessing qualifications for a particular job or task.
- ✓ Gathering evidence for disciplinary action or termination.
- ✓ Complying with applicable law.
- ✓ Education, training, and development requirements.
- ✓ Health administration services.
- ✓ Liaising with your pension provider.
- ✓ Complying with health and safety obligations.
- ✓ To ensure network and information security, including preventing unauthorised access
- ✓ to our computer and electronic communications systems and preventing malicious
- ✓ software distribution.
- ✓ Dealing with legal disputes involving you, or other employees, workers, and
- ✓ contractors, including accidents at work.
- ✓ To monitor your use of any company vehicles.
- ✓ To monitor your use of our information and communication systems to ensure
- ✓ compliance with our IT policies, to assist in the investigation of alleged wrongdoing (for example, during a disciplinary or grievance investigation), to find lost messages/emails/documents, or to comply with a legal obligation.
- ✓ To ensure network and information security, including preventing unauthorised access
- ✓ to our computer and electronic communications systems and preventing malicious
- ✓ software distribution.
- ✓ Assist in the running of our business.
- ✓ Comply with legal or regulatory requirements.
- ✓ Making decisions about your continued employment or engagement.
- ✓ Deciding for the termination of our working relationship.

We will only process your personal data for the purposes we collected it for or for compatible purposes. If we need to process your personal data for an incompatible purpose, we will provide notice to you and, if required by law, seek your consent. We may process your personal data without your knowledge or consent where required by applicable law or regulation. If you do not provide this personal data, we may be unable in some circumstances to comply with our obligations and we will tell you about the implications of that decision. Should we need to process your personal data for a purpose other than that which it was collected for, we will provide you with information on that purpose and any other relevant information. We may process your personal data for our own legitimate interests, including for the following purposes:

- ✓ To prevent fraud reporting potential crimes and to aid in the detection and prevention of crime.
- ✓ To ensure network and information security, including preventing unauthorized access to our computer and electronic communications systems and preventing malicious software distribution.
- ✓ To support internal administration with our affiliated entities.

- ✓ To conduct data analytics analyses to review and better understand employee retention and attrition rates.

We will process your data securely should any of the above arise.

We will use your personal data to perform checks required to do your job, for example we may need to conduct criminal records check as part of the employment process. We will only use information relating to criminal convictions where the law allows us to do so and in accordance with our data protection policy.
You may be referred to in company documents and records that are produced by you and/or your colleagues during the course of your employment and whilst doing business on behalf of the company.

To promote interdepartmental working and efficient working practices across the group we will publish your photographs on the intranet, this enables us to improve collaborative working and connections. We will use the photo taken on joining; you can change this picture at any time if you would like support with this please contact the Communications team. These photographs are for internal use only and a legitimate business use in line with current data protection legislations.

Collection and Use of Special Categories of Personal Data

The following special categories of personal data are considered sensitive under the laws of your jurisdiction and may receive special protection:

- ✓ Racial or ethnic origin.
- ✓ Political opinions.
- ✓ Religious or philosophical beliefs.
- ✓ Trade union membership.
- ✓ Genetic data.
- ✓ Biometric data.
- ✓ Data concerning health.
- ✓ Data concerning sex life or sexual orientation.
- ✓ Data relating to criminal convictions and offences may also receive special protection under the laws of your jurisdiction.

We may collect and process the following special categories of personal data when you voluntarily provide them for the following legitimate business purposes, to carry out our obligations under employment law, for the performance of the employment contract, or as applicable law otherwise permits:

- ✓ Trade union membership information for the purpose of paying trade union premiums.

- ✓ Physical or mental health information or disability status to comply with health and safety obligations in the workplace, to make appropriate workplace accommodations, as part of sickness absence monitoring, and to administer benefits.

- ✓ Race or ethnic origin, religious affiliation, health information and sexual orientation to ensure meaningful equal opportunity monitoring and reporting.

Where we have a legitimate need to process special categories of personal data for purposes not identified above, we will only do so only after providing you with notice and, if required by law, obtaining your prior, express consent.

We will always treat special categories of personal data as confidential and we will only share such data internally where there is a specific and legitimate purpose for sharing the data. We have implemented appropriate physical, technical, and organisational security measures designed to secure your personal data against accidental loss and unauthorised access, use, alteration, or disclosure.

We will only retain special categories of personal data for as long as necessary to fulfil the purposes we collected it for, as required to satisfy any legal, accounting, or reporting obligations, or as necessary to resolve disputes.

How we collect your personal data

The personal data we hold about you will have been provided by yourself during and after the recruitment process, we also collect personal data about you during your employment including from internal sources, such as your manager. In some cases, the data can come from external sources, such as referees, medical professionals, and government agencies like the Disclosure and Barring Service.

We may collect your personal data through monitoring your use of our computer systems. Our systems enable us to monitor telephone, email, voicemail, messages, internet and other communications. For business reasons, and to carry out legal obligations in our role as an employer, use of our systems including the telephone and computer systems, and any personal use of them, may be continually monitored. This might include, without limitation, the monitoring, intercepting, accessing, recording, disclosing, inspecting, reviewing, retrieving, and printing of transactions, emails, messages, communications, postings, and recordings. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes, and it will usually only be in specific circumstances with the permission of the Chief Executive or member of the Executive Committee. Please see our Information Security Policy for further information on monitoring your use of our computer systems.

Who we share your personal data with

We will not normally share your personal data without your consent unless the law allows or requires us to do so. Where it is legally required or necessary in accordance with data protection law, we may share employee personal data with:

- ✓ Our regulator.
- ✓ Other members of RHP.
- ✓ Suppliers and service providers.
- ✓ Financial organisations.
- ✓ Our auditors.
- ✓ Survey and research organisations.
- ✓ Trade unions and associations.
- ✓ Occupational health.
- ✓ Insurers.
- ✓ Pension providers.

- ✓ Professional advisers and consultants.
- ✓ Police forces, courts, tribunals.
- ✓ Professional bodies.
- ✓ Employment and recruitment agencies.
- ✓ Other businesses, if a business transfer or change in ownership occurs and the disclosure is necessary to complete the transaction. In these circumstances, we will limit data sharing to what is absolutely necessary, and we will anonymize the data where possible.
- ✓ Other individuals during emergency situations or where necessary to protect the safety of persons.
- ✓ With others where the personal data is publicly available.
- ✓ For additional purposes with your consent where such consent is required by law.

How we keep your data secure

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used, or accessed in an unauthorised way, altered, or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need-to-know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.

All personal data you provide to us is stored on our secure servers within the UK and is not transferred to other countries. However, there may be occasions where your data may need to be stored in or sent to companies, service providers, agents, subcontractors, and regulatory authorities in countries outside of the European Economic Area ('EEA') which may not have the same level of security and protection as we have under UK legislation. If we have to do this, we will make sure that suitable security measures are in place.

We have put in place procedures to deal with any suspected data security breach and will notify you and the Information Commissioner's Office of a suspected breach where we are legally required to do so.

How long we keep your data

We 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 used for determining how long your data will be stored for is detailed in the Employee Data Protection Policy. This can be found on our intranet and hardcopies can be requested from the People team.

We will keep your personal data for as long as you are an employee of the Group. After you stop being an employee, we may keep your data for up to 10 years for one of these reasons:

- ✓ To respond to any questions or complaints.
- ✓ To show that we treated you fairly.
- ✓ To maintain records according to rules that applies to us.

We may keep your data for longer than 10 years if we cannot delete it for legal or regulatory reasons.

Rights of Access, Correction, Erasure, and Objection

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 employment. By law you may have the right to request access to, correct, and erase the personal data that we hold about you, or object to the processing of your personal data under certain circumstances. You may also have the right to request that we transfer your personal data to another party. 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 the Data Protection and People teams (details below). Any such communication must be in writing.

We may request specific information from you to help us confirm your identity and your right to access, and to provide you with the personal data that we hold about you or make your requested changes. Applicable law may allow or require us to refuse to provide you with access to some or all of the personal data that we hold about you, or we may have destroyed, erased, or made your personal data anonymous in accordance with our record retention obligations and practices. If we cannot provide you with access to your personal data, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

If you want to exercise any of these rights, please contact us using the details in the (*Where to Get Help*) section below.

Right to Withdraw Consent

Where you have provided your consent to the collection, processing, or transfer of your personal data, you may have the legal right to withdraw your consent under certain circumstances. To withdraw your consent, if applicable, contact the Data Protection and People teams (details below).

Where to get help

Please contact us if you have any questions about our privacy notice or the information, we hold about you. You can do so via one of the contact details below.

- ✓ Email – dpo@rhp.org.uk and people@rhp.org.uk.
- ✓ Write to us - Data Protection Team and People Team, 8 Waldegrave Road, Teddington, Middlesex TW11 8GT.
- ✓ Call us – 08000322433.

We have also appointed a Data Protection Officer who is registered with the Information Commissioner's Office. Our Data Protection Officer can be contacted by emailing dpo@rhp.org.uk.

Alternatively, if you think our collection or use of personal information is unfair, misleading, or inappropriate or if you have concerns about the security of your personal information, you also have the right to make a complaint to the Information Commissioner's Office. You can contact the Information Commissioner's Office at the following address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Further information and guidance please visit https://ico.org.uk/concerns/.

The following documents also contain information regarding the Group's processing of personal data. Please also familiarise yourself with:

- ✓ Data Protection Policy
- ✓ Employee Data Protection Policy
- ✓ Data Subject Rights Policy
- ✓ CCTV Policy
- ✓ Document Retention Policy
- ✓ Information Security Policy
- ✓ Special Category Data Processing Policy
- ✓ Personal Data Breach Process.

The above documents are available via Lighthouse.

Our Employee Privacy Notice is regularly reviewed, and may change at any time in the future, we encourage you to check this privacy notice whenever you visit the intranet. Significant changes will be communicated to employees by email.