Atlantis Healthcare HR Privacy Notice

Atlantis Healthcare respects your right to privacy. This Privacy Notice explains who we are, how we collect, share and use personal data about you, and how you exercise your privacy rights. It applies to all prospective candidates, current and former employees, workers and contractors ("personnel"). This notice does not form part of any contract of employment or other contract to provide services.

It is important that you read this privacy notice together with any other privacy notice or fair processing notice we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data. **This privacy notice supplements the other notices and is not intended to override them.**

Atlantis Healthcare is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you.

1. Important Information

Who are we?

Atlantis Healthcare is made up of different legal entities, details of which can be found here. This privacy notice is issued on behalf of the Atlantis Healthcare Group of companies "Atlantis Healthcare" so when we mention Atlantis Healthcare, "we", "us" or "our" in this privacy notice, we are referring to the relevant company in the Atlantis Healthcare Group responsible for processing your data.

How to contact us

The data controller of your personal information will be the relevant Atlantis Healthcare entity with whom you are or were engaged.

Alternatively, if you have any questions about this privacy notice, including any requests to exercise your legal rights or concerns about our use of your personal information, please email us at privacy@atlantishealthcare.com

2. What personal information do we collect and why?

We will collect and process the following personal information about you:

- **Personal details:** your title, name, previous or maiden name, gender, nationality, civil/marital status, date of birth, age, personal contact details, national ID number, eligibility-to-work information, passport, driving licence, languages spoken; emergency contact information, details of any disability and any reasonable adjustments required as a result
- **Recruitment and selection information:** skills and experience, qualifications, references, CV and application, interview and assessment data, background and verification information related to the outcome of your application, details of any offer made to you
- **Information related to your engagement:** contract of employment or engagement, work contact details, employee or payroll number, photograph, work location, your worker ID and various system IDs, your work biography, your assigned business unit or group, your reporting line, your employee/contingent worker type, your termination/contract end date, the reason for termination, your last day of work, exit interviews
- **Regulatory information:** records of your registration with any applicable regulatory authority, your regulated status, including any criminal record or credit background checks which may be necessary, and any regulatory certificates and references.
- **Remuneration and benefits information:** your remuneration information (including salary/hourly plan/contract pay/fees information as applicable, allowances, overtime, bonus and commission plans), payments for leave/, bank account details, grade, tax information, details of any benefits you receive or are eligible for, benefit coverage start date, expense claims and payments, information and agreements
- **Leave and absence management information:** attendance records, absence records, holiday dates, requests and approvals and information related to family leave or other special or statutory leave, absence history, fit notes, details of incapacity, details of work impact and adjustments, manager and Human Resources (HR) communications, return to work interviews. In New Zealand, AAC and application for Domestic Violence Leave and all other locally specific applications
- **Performance management information:** colleague and manager feedback, your appraisals and performance review information, outcomes and objectives, talent programme assessments and records, succession plans, formal and informal performance management process records
- **Training and development information:** data relating to training and development needs or training received, or assessments completed
- **Monitoring information (to the extent authorised by applicable laws):** closed circuit television footage, system and building login and access records, photo on access card, download and print records, call or meeting recordings, information captured by IT security programmes and

filters

- **Employee claims, complaints and disclosures information:** subject matter of employment or contract based litigation and complaints, pre claim conciliation, communications, settlement discussions, claim proceeding records, employee involvement in incident reporting and disclosures
- **Equality and diversity information (where authorised by law and consent provided voluntarily):** information regarding gender, age, nationality, religious belief, sexuality and race (stored anonymously for equal opportunities monitoring purposes)

We will only use your personal information when the law allows us to. Most commonly, we will use your personal data for at least one of the following circumstances:

- where we need the personal information to perform a contract with you;
- where we have a legal or regulatory obligation to do so;
- where the processing is in our legitimate interests and not overridden by your data protection interests or fundamental rights and freedoms.

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

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest or for official purposes.

The purposes and legal bases are listed below:

Purpose	Legal Basis
Making a decision about your recruitment or appointment. CV, references, covering letter, application form, interview sheets, pre-employment form, results from assessment tests, visa status, LinkedIn and other social media websites	Performance of a contract with you
Determining the terms on which you work or contract for us	Performance of a contract with you
Checking you are legally entitled to work or contract in the country in which you are employed or are contracting	Legal or regulatory obligation
Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and social security/National Insurance contributions (NICs), and other local schemes etc	Performance of a contract with you
Providing any of the following benefits to you: carpark, bonus, superannuation / benefits scheme, medical insurance, indemnity insurance, travel insurance, etc	Performance of a contract with you

Purpose	Legal Basis
Inviting you to participate in any share plans operated by a group company	Performance of a contract with you
Granting awards under any share plans operated by a group company	Performance of a contract with you
Administering your participation in any share plans operated by a group company, including communicating with you about your participation and collecting any tax and NICs due on any share awards	Performance of a contract with you
Enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties	Legal or regulatory obligation
Liaising with the trustees or managers of a pension arrangement operated by a group company, your pension provider and any other provider of employee benefits	Performance of a contract with you
Business management and planning, including accounting and auditing	Legitimate Interests
Conducting performance reviews, managing performance and determining performance requirements	Legitimate Interests
Making decisions about salary reviews and compensation	Legitimate Interests
Assessing qualifications for a particular job or task, including decisions about promotions	Legitimate Interests
Gathering evidence for possible grievance or disciplinary hearings	Legal or regulatory obligation
Making decisions about your continued employment or engagement	Legitimate Interests
Making arrangements for the termination of our working or contracting relationship	Legitimate Interests
Education, training and development requirements and historical records	Legitimate Interests

Purpose	Legal Basis
Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work	Legal or regulatory obligation
Ascertaining your fitness to work	Legitimate Interests
Managing sickness absence	Legitimate Interests
Complying with health and safety obligations	Legal or regulatory obligation
To prevent fraud	Legal or regulatory obligation
To monitor your use of our information and communication systems to ensure compliance with our IT policies	Legitimate Interests
To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution	Legitimate Interests
To conduct data analytics studies to review and better understand core HR metrics, employee retention and attrition rates	Legitimate Interests
Equal opportunities monitoring	Legitimate Interests
To gather employee feedback about induction, levels of engagement and culture, exit interviews, turnover, and all other HR metrics	Legitimate Interests

In general, we will not process particularly sensitive personal information about you unless it is necessary for performing or exercising obligations or rights in connection with employment or contracting. 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 information are listed below.

- We will use information about your physical or mental health, ACC claim, or disability status to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits including statutory maternity pay, statutory sick pay, pensions and permanent health insurance We need to process this information to exercise rights and perform obligations in connection with your employment. In the case where an applicant is unsuccessful data, such as this would be destroyed within 2 weeks of the role being successfully filled.

- The collection of material described in previous paragraph will only apply in markets where local HR legislation permits this. In cases where it does not, e.g. Germany, local HR legislation will be adhered to both in terms of collection of data during a candidate's application process and storage of such information once they become an employee. In the case of Germany, mutual consent would be required prior to storage of such information.
- If you leave employment and under any share plan operated by a group company the reason for leaving is determined to be ill-health, injury or disability, we will use information about your physical or mental health, or disability status in reaching a decision about your entitlements under the share plan.
- If you apply for an ill-health pension under a pension arrangement operated by a group company, we will use information about your physical or mental health in reaching a decision about your entitlement.
- We will use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.
- Workplace requirements such as altered work hours, physical workplace aids e.g. special chairs etc specific to an individual implemented to reduce harm and optimise comfort in cases of a pre-existing medical condition. In the event that a national workplace safety body is involved, data may need to be shared to ensure rehabilitation is progressing.
- Medical conditions and associated medic alert (or similar) details in case of emergency treatment being required in the workplace shared with supervisors and First Aid staff members e.g. insulin dependent diabetes, severe allergies etc.

If you fail to provide personal information

If you fail to provide information when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to process your application successfully. For example, if we require a credit check or references for this role and you fail to provide us with relevant details, we will not be able to take your application further.

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers or contractors).

Change of purpose

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 and permitted by law.

3. 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 envisage that we will hold information about criminal convictions as required by client contracts or specific role requirements.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences in the following ways:

- To assess suitability for a role
- To determine whether the employment or contracting relationship is continued in the event that a serious criminal conviction is issued during the time of employment or contracting at Atlantis Healthcare

We are allowed to use your personal information in this way to carry out our obligations where clients demand a clean criminal conviction record and any criminal conviction is fully disclosed and considered prior to or during employment in the event this occurs after employment has started. We have in place an appropriate policy and safeguards which we are required by law to maintain when processing such data.

4. How do we collect your personal information?

We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies, psychometric testing agencies or other background check agencies.

We may also collect personal information from the trustees or managers of pension arrangements operated by a group company.

We will collect additional personal information in the course of job-related activities throughout the period of you working or contracting for us.

5. When and with whom might we share your personal information?

We may share your personal information with:

- the Atlantis Healthcare group of companies for the purposes connected with your employment or the management of our business;
- third parties for the purposes of complying with our contractual duties to you, for instance as payroll providers, HR and Learning and Development (L&D) platform providers, and benefit providers;
- a potential buyer (and its agents and advisers) in connection with any proposed purchase, merger or acquisition of any part of our business, provided that we inform the buyer it must use your personal information only for the purposes disclosed in this Privacy Notice.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their

own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

We will not share your personal information any company outside the Atlantis Healthcare group of companies for marketing purposes.

6. Disclosures of your personal data

In certain circumstances, we may disclose your personal information with competent law enforcement bodies, regulators, government agencies, courts or other third parties without your knowledge or consent for the following purposes:

- The prevention or detection of crime;
- The apprehension or prosecution of offenders;
- The assessment or collection of a tax or duty;
- By the order of a court or by any rule of law

7. International transfers

Atlantis Healthcare operates in the UK, EU and around the world. This means that when we collect your personal information it may be processed in countries that may have data protection laws that are different to the laws of your country.

However, we have taken appropriate safeguards to require that the personal information we process will remain protected in accordance with this Privacy Notice when transferred internationally, including when processed internationally by our third party service providers and partners.

If you have questions about, or need further information concerning, international data transfers, please send an email to privacy@atlantishealthcare.com

8. How does Atlantis Healthcare keep my personal information 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.

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

9. Data retention

We will only retain your personal information 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.

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.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

Once you are no longer an employee, worker or contractor, or have been unsuccessful in your job application, of the company we will retain and securely destroy your personal information in accordance with our data retention policy and any applicable laws and regulations.

If you have questions about, or need further information concerning our data retention periods, please contact your local HR representative.

10. Your legal rights & obligations

Under certain circumstances, by law you have the right to:

- Right to be informed about the processing of your personal data
- Right to rectification if your personal data is inaccurate or incomplete (requests to amend data will normally have to be processed within 1 month)
- Right of access to your personal data and supplementary information, and the right to confirmation that your personal data is being processed
- Right to be forgotten by having your personal data deleted or removed on request where there is no compelling reason for an organisation to continue to process it again (employers will have to respond without undue delay or and within 1 month of the request)
- Right to restrict processing of your personal data, for example, if you consider that processing is unlawful, or the data is inaccurate
- Right to data portability of your own personal data for your own purposes (you will be allowed to obtain and reuse your data)
- Right to object to the processing of your personal data for direct marketing, scientific or historical research, or statistical purposes

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party please email privacy@atlantishealthcare.com

We respond to all requests received from individuals wishing to exercise their data protection rights in accordance with applicable data protection laws. However, we may not always be able to comply with your request for specific legal reasons which will be notified to you, if applicable, at the time of your request.

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

We may also contact you to ask you for further information in relation to your request to speed up our response.

You have the right to complain to a data protection authority about our collection and use of your personal information. For more information, please contact your local data protection authority.

- Contact details for data protection authorities in the European Economic Area, Switzerland and certain non-European countries (including the US and Canada) are available here
- Contact details for the data protection authority in the UK are available here
- Contact details for the data protection authority in New Zealand are available here
- Contact details for the data protection authority in Australia are available here
- The USA has no single national data protection authority. The FTC has jurisdiction over most commercial entities and has authority to issue and enforce privacy regulations in specific areas (for example telemarketing, commercial email, and children's privacy) and to take enforcement action to protect consumers against unfair or deceptive trade practices, including materially unfair privacy and data security practices. Many state attorneys general have similar enforcement authority over unfair and deceptive business practices, including failure to implement reasonable security measures and violations of consumer privacy rights that harm consumers in their states. The California Attorney General has the authority to enforce the CCPA and most California consumer privacy laws. In addition, a wide range of sector-specific regulators, particularly those in the healthcare, financial services, telecommunications and insurance sectors, have authority to issue and enforce privacy and security regulations, with respect to entities under their jurisdiction.

Your duty to inform us of changes

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 your working relationship with us. This is a requirement from a business continuity perspective so that in the event of emergency your details are current.

Last Updated: March 2021