|  |
| --- |
| **1. WHAT IS THE PURPOSE OF THIS PRIVACY STATEMENT?** |
| 1.1    Under the UK GDPR and Data Protection Act 2018, we are required to explain to you why we collect your information, how we intend to use that information and whether we will share this information with anyone else. This statement applies to all current and former employees.  1.2    This statement does not form part of any contract of employment or other contract to provide services.  1.3.    It is important that you read this Privacy Statement for Employees so that you know how and why we use your information. We may update this Privacy Statement for Employees at any time.  1.4    It is also important that you inform us of any changes to the personal information we hold about you so that the information is accurate and up to date. |

|  |
| --- |
| **2. WHO ARE WE?** |
| 2.1    We are Tinkers Hatch Care Home Limited (Tinkers Hatch), a company registered in England and Wales under company number 5894476 and with our registered office at 39 High Street, Battle, East Sussex, TN33 0EE.   2.2    Tinkers Hatch is the "Data Controller" for the information which we hold about you. This means that we are responsible for deciding how and why we hold your personal information. |

|  |
| --- |
| **3. OUR DATA PROTECTION OFFICER** |
| 3.1    Our Data Protection Officer (DPO) is responsible for overseeing what we do with your information and monitoring our compliance with the Data Protection Laws.  3.2    Our DPO is Dean Webber who is assisted by the Compliance Officer – Rebecca Vine. If you have any concerns or questions about our use of your personal data, you can contact raise these by emailing dean.webber@Tinkershatch.co.uk or writing to Tinkers Hatch, New Pond Hill, Cross in Hand, Heathfield, TN21 0LX – FAO DPO. Alternatively, if you wish to make contact but are unable to use any of the above methods, please contact your Key Worker who will be able to put your queries forward to the team. |

|  |
| --- |
| **4. TYPES OF PERSONAL INFORMATION WE USE AND OUR LAWFUL BASIS FOR DOING SO** |
| 4.1    We process your personal information for a number of reasons. If you refuse 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 employees). If this is the case, we may be required to terminate your contract of employment.  4.2    In accordance with the Data Protection Laws, we need a lawful basis for collecting and using information about you. These lawful bases are set out in Article 6 of the UK GDPR and, depending on the type of data, may require reliance on additional safeguards set out in Articles 9 and 10 of the UK GDPR and within the Data Protection Act 2018.  Standard personal data:  4.3    We will process standard personal data about you. Please refer to the **Appendix** to see the types of data we might process about you. 4.4    Our Article 6 UK GDPR lawful bases for processing this type of data are:  4.4.1    You have given us **clear consent** to process your personal data (in the circumstances where consent is the only available lawful basis) (Article 6(1)(a)) of the UK GDPR); or 4.4.2    It is necessary in order for us **to perform our contract with the client/you** (Article 6(1)(b) of the UK GDPR); or 4.4.3    It is necessary **to meet legal / regulatory obligations** (Article 6(1)(c) of the UK GDPR); or 4.4.4    It is necessary for our**legitimate interests** (where they are not overridden by your rights) (Article 6(1)(f) UK GDPR). Special categories of personal data:  4.5    Some of the information which we may process about you will be “special category personal data” and criminal activity data. Special category personal data and criminal activity data (see further below) require a greater level of protection than standard personal data. Please refer to the **Appendix** to see the types of special category personal data and criminal activity data we might process about you.  4.6    Our Article 6 UK GDPR lawful bases for processing this type of data are:  4.6.1    You have given us **consent** to process your personal data (in the circumstances where consent is the only available lawful basis) (Article 6(1)(a)) of the UK GDPR); or 4.6.2    It is necessary in order for us **to perform our contract of employment with you** (Article 6(1)(b) of the UK GDPR); or 4.6.3    It is necessary **to meet legal / regulatory obligations** (Article 6(1)(c) of the UK GDPR); or 4.6.4    It is necessary **to protect your life** (Article 6(1)(d) of the UK GDPR); or 4.6.5    It is necessary for our **legitimate interests** (where they are not overridden by your rights) (Article 6(1)(f) UK GDPR). 4.7    We also require an Article 9 UK GDPR basis and must meet other additional conditions specified within the Data Protection Act 2018 to process this type of data.  Criminal activity data:  4.8    We may process information about you in relation to details of criminal activity in relation to proven and unproven criminal offences (including allegations of criminal activity, investigations into criminal activity, details of proceedings and outcomes of proceedings). Please refer to the **Appendix**for more details of the data we might process about you.  4.9    Our Article 6 UK GDPR lawful bases for processing this type of data are:  4.9.1    You have given us **consent** to process your personal data (in the circumstances where consent is the only available lawful basis) (Article 6(1)(a)) of the UK GDPR); or 4.9.2    It is necessary in order for us **to perform our contract with the client/you** (Article 6(1)(b) of the UK GDPR); or 4.9.3    It is necessary **to meet legal / regulatory obligations** (Article 6(1)(c) of the UK GDPR); or 4.9.4    It is necessary for our **legitimate interests** (where they are not overridden by your rights) (Article 6(1)(f) UK GDPR). 4.10    We also require an additional Article 10 UK GDPR condition for processing this type of data, and must meet other additional conditions specified within Schedule 1 of the Data Protection Act 2018 to process this type of data. |

|  |
| --- |
| **5. SOURCE OF YOUR PERSONAL INFORMATION** |
| 5.1    The information described at paragraph 4 which we collect about you will be obtained through a variety of sources which may include:  5.2 5.2.1    from you directly as part of the recruitment process and during the course of and after your employment with us (including information volunteered by you); 5.2.2   from third parties as part of the recruitment process (such as employment agencies, background check providers, former employers, credit reference agencies and agency companies); 5.2.3    information obtained about you in the course of job-related activities throughout the period of your employment with us;  5.2.4    information which you have otherwise made public; 5.2.5    from external healthcare providers such as the NHS, your GP, hospital staff, dentists etc; 5.2.6    from safeguarding authorities / commissioning bodies and Integrated Care Boards / other regulators (such as the Nursing and Midwifery Council and the Information Commissioner’s Office) (and in some circumstances, their professional advisors or authorised representatives); 5.2.7    from the Police and other law enforcement agencies (for example, the Home Office), the courts, the Office of the Public Guardian and coroners; 5.2.8    from professional advisors (including solicitors and insurers); 5.2.9    from social media activity (such as Facebook, Linkedin etc.); 5.2.10    from other entities/persons which fall outside of this list which is made known to us relation to your employment or your right or fitness to work; and 5.2.11    Because circumstances are variable and change with time there may in some instances be situations outside the list above and we regularly review our Privacy Statement for Employees to assess whether any updates are required. |

|  |
| --- |
| **6. COMPLYING WITH DATA PROTECTION LAW** |
| 6.1    We will comply with the Data Protection Laws when using your personal information. At the heart of the Data Protection Laws are the data protection principles (Article 5(1) of the UK GDPR) which say that the personal information we hold about you must be:  6.1.1    processed lawfully, fairly and in a transparent way; 6.1.2    collected only for specified, explicit and legitimate purposes and not used in any way that is incompatible with those purposes; 6.1.3    adequate and relevant to the purposes we have told you about and limited only to those purposes; 6.1.4    accurate and, where necessary, kept up to date; 6.1.5    kept only as long as necessary for the purposes we have told you about; and 6.1.6    processed in a manner that ensures appropriate security. |

|  |
| --- |
| **7. SHARING YOUR INFORMATION** |
| 7.1    We will share your personal information with third parties where we have a lawful basis for doing so.  7.2    The types of organisations/persons with which we may share your personal data are as follows:  7.2.1    External healthcare providers such as your GP, hospital staff, dentists, other care providers etc; 7.2.2    Safeguarding authorities / commissioning bodies and Integrated Care Boards / other regulators (such as the Nursing and Midwifery Council and the Information Commissioner’s Office) (and in some circumstances, their professional advisors or authorised representatives). 7.2.3    The Police and other law enforcement agencies (for example, the Home Office), the courts, the Office of the Public Guardian and coroners. 7.2.4    IT service providers: we may use external IT or software providers who may have access to your personal data from time to time as is necessary to perform their services. 7.2.5    Auditors / professional advisors (including solicitors and insurers). |

|  |
| --- |
| **8. TRANSFERING INFORMATION OUTSIDE OF THE UK AND THE EUROPEAN ECONOMIC AREA (EEA)** |
| 8.1    We strive to ensure that any data necessary to be shared with the companies we work with (i.e. our supply chains) remains within the UK or the EEA in the first instance. However, some companies that provide services to us are located in, or run their services from, countries outside of these areas and resultantly, on occasion, your personal data may be transferred to countries outside of these areas. |

|  |
| --- |
| **9. CAN WE USE YOUR INFORMATION FOR ANY OTHER PURPOSE?** |
| 9.1    We typically will only use your personal information for the purposes for which we collect it. It is possible that we will use your information for other purposes as long as those other purposes are compatible with those set out in this Privacy Statement for Employees. If we intend to do so, we will provide you with information relating to that other purpose before using it for the new purpose. |

|  |
| --- |
| **10. STORING YOUR INFORMATION AND DELETING IT** |
| 10.1    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 only retain your personal information in line with periods calculated using such criteria and in consideration of how long it is reasonable to keep records to show we have met the obligations we have to you and by law, any time limits for making a claim, any periods for keeping information which are set by law or recommended by regulators, professional bodies or associations.  10.2    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. |

|  |
| --- |
| **11. YOUR RIGHTS** |
| 11.1    Under certain circumstances, you have the right to: 11.1.1    Request access to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.  11.1.2    Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected. 11.1.3    Request erasure of your personal information in certain circumstances. This enables you to ask us to delete or remove personal information 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 information where you have exercised your right to object to processing (see below). 11.1.4    Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) or public interest as our lawful basis for processing and there is something about your particular situation which leads you to object to processing on this ground. You also have the right to object if we are processing your personal information for direct marketing purposes. 11.1.5    In the limited circumstances where we are relying on your consent as our lawful basis to process your data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. If you withdraw your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another lawful basis for doing so. 11.1.6    Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it. 11.1.7    Request the transfer of your personal information to another party.  11.2    If you wish to exercise any of the above rights, please contact our Data Protection Officer whose details are set out in Section 3. |

|  |
| --- |
| **12. AUTOMATED DECISION MAKING** |
| 12.1    You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making. |

|  |
| --- |
| **13. RIGHT TO COMPLAIN TO THE ICO** |
| 13.1    You have the right to complain to the Information Commissioner's Office (the "ICO") if you are not satisfied with the way we use your information. You can contact the ICO by writing to Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF or ico.org.uk. |

|  |
| --- |
| **14. CHANGES TO THIS PRIVACY STATEMENT** |
| 14.1    We reserve the right to update this Privacy Statement for Employees at any time where appropriate. |

|  |
| --- |
| **15. APPENDIX** |
| 1. 1. The standard personal data we may process about you includes:  - personal details (such as name, date of birth, gender, nationality, marital status, national insurance number), contact details (such as your address, personal telephone number and personal email address), and confirmation of your identity (such as a copy of your passport, birth certificate, driving licence) in order to confirm your identity, for recruitment and ongoing employment purposes, to allow us to assess that you are a fit and proper person to work for us and for the purposes of communicating with you before, during and after your employment with us for reasons connected to your employment;   - recruitment information (such as copies of right to work documents, references and other information included in a CV/job application form or cover letter or as part of the application process) in order for us to assess your lawful right to work in the UK and for statistical and equal opportunities monitoring purposes;   - information about your family and others (such as dependants, next of kin and emergency contact numbers) so we know who to contact if there is an emergency;   - details and evidence of professional qualifications (for example, if you are a nurse, your NMC PIN number) so we can verify these are required for your job role and to ensure you are a fit and proper person to work within that role;   - information relating to your remuneration (such as bank account details, payroll records, tax status information, salary history, pension and benefits, information about your previous employment (such as job titles, work history, working hours, training records, professional memberships, salary / compensation history) so that we are able to pay and provide any benefits to you, as well as deducing National Insurance contributions, for the purposes of fulfilling our requirements in respect of your pension and for making decisions about your salary;   - information about your employment with us (such as start date, location of employment / workplace) and your performance with us (such as appraisal information, colleague and customer feedback, etc) or complaints or made about your performance so as to allow us to conduct performance reviews and determine any necessary performance/training requirements; to allow us to carry out any necessary disciplinary processes or provide evidence for legal proceedings (including instigating or responding to any claims) and for safeguarding and regulation of care purposes, including responding to complaints;   - disciplinary and grievance information (including with any third party organisations, such as the Nursing and Midwifery Council);   - security information images/audio of you (such as CCTV footage, swipecard information, etc) and photographs in order to ensure public safety i.e. the safety and security of our clients and employees and those who visit our premises, as well as identify and help to deter criminal activity (such as vandalism/damage to the property and theft) and create an overall secure living and working environment;   - information about your use of our information and communications systems/electronic devices, including the monitoring of your use of our information and communication systems to ensure compliance with our IT and data protection policies as may be in place from time to time, in order 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.   - information about your day to day activities and for administrative functions which are necessary for the day to day functioning of our organisation, including the prevention, detection and investigation of fraud and corruption, and the administration of the contract we have entered into with you, regulatory referrals, business management and planning, including accounting and auditing;   - we may also process your data by sending you email or text message communications in relation to your employment/the business and ask for your views on the ways in which we could improve our services and improve the employment environment pursuant to our contact with you.   - We may also ask for your consent for information about you to be featured in our marketing material, including (but not limited to) brochures and other such printed and electronic publications, the Tinkers Hatch website and social media pages and other promotional pages linked to Tinkers Hatch; and   - because circumstances are variable and change with time, there may in some instances be situations outside the list above, and we regularly review our privacy statements to assess whether any updates are required.  2.     The special category personal data which we may process about you (in order to provide you with safe, appropriate and personalised care and accommodation) includes the following: 2. - information about your racial or ethnic origin; - information about your religious beliefs;   - information about your sex life and sexual orientation and political opinions; and   - trade union membership (in order to make trade union premiums);   - information about your health, including any disabilities or special requirements which you may have, medical condition or disability, health and sickness records applying to the time you have spent with us, your medical history, vaccination status and history, (in order to allow us to make workplace adjustments, to ensure your health and safety and the health and safety around you within the workplace and to assess your fitness to work, monitor and manage sickness absence and to administer benefits);   - biometric data (such as your fingerprint, face or audio recognition) in order to log into verify your identity to log in to company systems, or test data (for example, Covid-19 swab test data);  3.     We may process criminal activity data about you. This may include information in relation to allegations of criminality, investigations and proceedings. We will only this type of information if it is appropriate given the nature of the role and where we are legally able and / or required 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/others in the course of you working for us. We will use information about criminal convictions and offences in the following ways: 3. - To assess whether you are a fit and proper person to work for us.   - To protect our clients/others within the workplace from the risk of assault, abuse, theft or possession or any other detriment at the hands of unsuitable employees.   - We have a duty of care to ensure that the people we employ have no history that would indicate they are unsuitable to work with vulnerable people.   - We are allowed to use your personal information in this way to carry out our obligations as your employer and because it is necessary to meet legal / regulatory obligations.   - Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary 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.   - We may also process such information in the course of legitimate business activities with the appropriate safeguards. |