Privacy and Fair Processing Notice

Employees and workers

Anyone that works with us at the Superior Healthcare Group can rest assured that we value your privacy and want you to understand the choices and control you have over your information we hold about you. We have created this GDPR Privacy Notice to help explain those choices and give you that control.

This Privacy and Fair Processing Notice ('notice') applies to prospective, current and former employees, workers, contractors, agency staff, jobseekers and volunteers (referred to as 'you' or 'your') and it is important that you read through it carefully.

1. Definitions

- The General Data Protection Regulations (GDPR) have recently come into force, and these regulations mean companies need to be clear about how they obtain and use personal data.
- In order to implement and comply with GDPR you are being given this notice to inform you about how and why we process personal data and the lawful basis for doing so.
- The Superior Healthcare Group Ltd ('we' or 'us') is a 'data controller' for the purposes of data protection legislation. A data controller determines the purposes and means of processing personal data.
- Personal data is any information which relates to an individual who can be identified from that information.
- Processing includes the collection, recording, storage, use, disclosure or destruction of personal data.
- This notice describes the categories of personal data we use during our recruitment process and throughout your employment and working with us, and the legal basis on which we do this, and for what purpose.
- This notice does not provide exhaustive detail. However, we are happy to provide any additional information or explanation needed. Any requests for this should be addressed to our Data Protection Officer (see Section 14).

2. General Data Protection Regulations

The GDPR principles are as follows:

- **Lawfulness, fairness and transparency** – data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- **Purpose limitation** – data must be collected only for specified, explicit and legitimate purposes.
- **Data minimisation** – data must be adequate, relevant and limited to what is necessary.
- **Accuracy** – data must be accurate and, where necessary, kept up to date. Inaccurate data must be erased.
- **Storage limitation** – data must only be stored for as long as is necessary.
- **Integrity and confidentiality** – data must be processed in a secure manner.
- **Accountability** – the data controller is responsible for, and must be able to demonstrate, compliance with the other data protection principles.

3. What personal information do we collect?

The collection and processing of personal data is necessary in order that we can enter a contract with you to provide services for the organisation. If you fail to provide the details requested, we may be unable to comply with the terms of any contract with you or comply with our legal obligations to you.

We may process the following categories of personal data about you:

- Name, address, contact details, date of birth (in order to enter into your contract of employment you are required to provide your personal details. If you do not provide this information, we will not be able to employ you).
- Terms and conditions of employment.
- Qualifications and work experience as set out in job applications and CVs.
- Bank account details and national insurance number (in order to enter into your contract of employment you are required to provide bank details and your national insurance number to the organisation. If you do not provide this information, we will not be able to process payments to you and account for tax and national insurance deductions to HMRC which we are required to do by law).
- Pensions scheme membership details (you are required under the terms of your contract to provide information about your pension scheme membership. If you do not provide this information, we will not be able to administer your pension benefits).
- Information about your right to work in the UK (in order to enter into your contract of employment, you are legally required to provide evidence of your right to work in the UK. If you do not provide this information, we will not be able to employ you).
- Information about criminal offences (in order to enter into your contract of employment, you may be required to provide information and agree to undertake a DBS check to enable us to confirm that you have no relevant unspent convictions or other factors that may put our service users at risk and to verify your suitability for the position. If you are required to and do not provide this information, we will not be able to employ you).
- Periods of leave which are requested and which have been taken, like: annual leave and sickness absence, maternity, paternity, parental leave (you are required under the terms of your contract and you are obliged under statute to provide information about periods of leave. We require this information to provide you with your statutory and contractual benefits. If you do not provide this information, we may not be able to provide these benefits).
- Disciplinary and grievance procedures including warnings.
- Records of appraisals and performance improvement plans.
- Special category data:
    - Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
    - Trade union membership.
    - Information about your health, including any medical condition, health and sickness records and data about immunisations and vaccinations.
- Your use of our IT, communication and other systems including internet searches.
- Details of your use of social media,.
- Details in references about you that we give to others.

4. How do we obtain your personal information?

4.1 Personal data about you is collected in many ways:

- through direct communications with you either face to face or in writing, email or on the telephone;
- through monitoring of our websites and our computer networks and connections;
- CCTV and access control systems;
- communications systems, remote access systems;
- from your doctors, from medical and occupational health professionals we engage;
- email and instant messaging systems;
- clearance procedures for working in the NHS and other clients.

- intranet and internet facilities.

4.2 In some cases, Superior Healthcare Group collects personal data about you from third parties, such as references supplied by former employers, information from employment background check providers, information from credit reference agencies and information from criminal records checks permitted by law. We aim to ensure that our data collection and processing is always proportionate. We will notify you of any material changes to information we collect.

5. What are the legal grounds for us processing your personal information?

5.1 We process your personal data for employment purposes and to provide an effective service to our clients. We will only use your personal data when the law allows us to and processing is necessary.

5.2 The most common legal bases for processing your personal data that we rely upon are:

- Where processing is necessary for the performance of a **contract** through which you are engaged. For example, employment contracts, contracts for services, contracts with CCGs and directly with private clients.
- Where processing is necessary to comply with a **legal obligation**. For example Employment law acts, Immigration acts, Health and Safety Acts, Equality Act etc.
- Where it is necessary for our **legitimate interests** (or those of a third party) and your interests and fundamental rights do not override those interests. For example for proper performance of our business.
- Where processing is necessary for the performance of a task carried out in the **public interest**. For example, we would have duty to disclosure your personal information if requested by one the Police Force or Home Office etc or a client such as the NHS in relation to safe and effective provision of healthcare.

6. Consent

6.1 Occasionally we may need your consent to use your personal information (for marketing communication, for example). However, as above, generally we won't need your consent to use personal information – for example if we need it to meet regulatory requirements or if it is necessary for an effective performance of your contract.

6.2 Where you provide consent to the processing of your data, you should be aware that you will be able to withdraw your consent at any time.

7. Special category data

7.1 We will only process special category data about genetic and biometric data, and data regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, and sexual orientation, where a further condition is also met. The conditions which will usually apply are that we have a legal obligation to process the information, where it is necessary in the public interest or to assess your working capacity on health grounds or, less commonly, where it is needed in relation to legal claims.

7.2 We may use your special category data in the following ways:

- information relating to leaves of absence, which may include sickness absence or family related leave, to comply with employment and other laws.
- information about your physical or mental health, 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.

- information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.
- For the safety and security reasons we will use your photograph for the purpose of the production of a Superior Healthcare Group Staff Identification Card as well as the Staff Personal Profile and to comply with legitimate requests of our clients e.g. NHS in relation to ID requirements.

8. Criminal offence data

8.1 The CQC requires that we, as CQC-regulated service providers, carry out DBS checks where we are authorised to do so under legislation. You should be aware that certain roles will require either a standard, enhanced or enhanced with barred list information DBS check to be carried out.

8.2 We will only require a DBS check to be made where the role is eligible and the check shall be at the appropriate level only and no higher.

8.3 We will assess the relevance of any cautions and convictions detailed in the DBS check to the role for which the applicant has applied.

8.4 Given the sensitive nature of the information contained in a DBS certificate, we will ordinarily only retain on file information about the level of check which was requested, the number of the disclosure certificate and the date on which the certificate was obtained.

9. Where do we store this information?

9.1 We store your information on a number of technology-based systems, such as emails and databases which help us to provide an efficient service to you. On commencement of employment or work with us, your personal data will be uploaded to the electronic People Planner database system and Sage payroll system which are HR and payroll solutions used by us for management purposes.

9.2 Your information will also be held in controlled paper-based filing systems at our Head Office, occasionally (normally at the recruitment stage) at our local offices and on our protected network with regards to computer-based documents.

9.3 In order to access the information ourselves or provide details to statutory authorities, we keep information for 6 years after your employment has ceased.

10. Retention periods

10.1 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.

10.2 Retention periods for personal data will vary according to 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.

10.3 Employee/ worker documentation will ordinarily be retained for **six years** after termination of employment, which is the statutory limitation period for breach of contract claims, and then promptly deleted once that period has passed.

10.4 For unsuccessful job candidates, documentation is retained for **six months** after he or she is rejected for a role, and then deleted.

11. Who do we share this information with?

11.1 Your information will be shared internally, including with members of the HR, Payroll and Recruitment teams, your line manager, coordination team and relevant authorised (normally senior) head office team members and IT staff if access to the data is necessary for performance of your role.

11.2 Superior Healthcare Group also shares your data with third parties in order to obtain pre-employment references (i.e. from other employers), obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service.

11.3 Superior Healthcare Group may also share your data with third parties in the context of a sale of some or all of its business or a TUPE transfer e.g. in the event of a change of contract provider. Such sharing of data will be subject to confidentiality arrangements.

11.4 Superior Healthcare Group also shares your data with third parties that process data on our behalf, in connection with payroll, the provision of benefits or training and the provision of occupational health services.

11.5 Superior Healthcare Group may also share your data with our clients, to demonstrate that all the required compliance checks have been completed and that you have received all the mandatory training and have the right skills to perform your role. This will usually include sharing your name, details of your compliance checks (references, DBS certificate date), details of your training and a summary of your skills and employment history.

11.6 Superior Healthcare may be also required to comply with our contractual obligations towards our clients and we may be asked to provide your personal data for auditing purposes. This means that external auditors may access your personnel file to ensure our compliance with the legislation and our contractual obligations.

11.7 We require third parties to respect the security of your data and to treat it in accordance with the law. We will share your personal information 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.

11.8 All our third-party service providers and other entities are required to take appropriate security measures to protect your personal information 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.

11.9 We will not transfer your data to countries outside the European Economic Area.

12. Automated decision making

12.1 An automated decision is one that is made with no human involvement. For example, your occupational health questionnaire will initially go through an automated process to determine your fitness to work. However, should the outcome be anything other than a positive one, this will be reviewed by an Occupational Health practitioner before any further action and a final decision is reached.

12.2 Please be aware that you will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

13. Rights of access, correction, erasure, restriction and portability

13.1 You have the following rights under the GDPR:

- Request **access to your personal data** (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.
- Request **correction of the personal data** that we hold about you. This enables you to ask to have any incomplete or inaccurate information we hold about you corrected.
- Request **erasure** of your personal information. 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 may exercise your right to have your personal data erased in a number of circumstances (e.g. if the data is no longer necessary in relation to the purpose for which it was created or you withdraw your consent).
    - Where possible we will comply with all such requests, though some details are part of the Superior Healthcare Group's permanent records (e.g. historical salary, expenses paid) which cannot reasonably be deleted.
    - Data we hold for statutory purposes such as Tax and Pensions cannot be deleted by law and we will comply with statutory retention periods for such data.
- **Object to processing** of your personal information on grounds relating to your particular situation where we are relying on a legitimate interest (or those of a third party) or where processing is necessary for the performance of a task carried out in the public interest as the lawful basis for processing.
- **Request the restriction** of processing of your personal information on the following grounds:
    - you contest the accuracy of the personal data for a period enabling us to verify the accuracy;
    - the processing is unlawful and you oppose the erasure of the personal data and requests restriction instead;
    - we no longer need the personal data for the original purposes of the processing, but the data is required by you for the establishment, exercise or defence of legal claims.
- **Request the transfer** of your personal information to another party, also known as portability.

13.2 Please contact our Data Protection Officer in writing (contact details below) if you would like to exercise any of your rights under the GDPR. We will aim at responding to you within 30 calendar days of our receipt of your request.

13.3 To help us deal with your request as efficiently as possible, you will need to include:

- Your current name and address
- Proof of identity (a copy of your driving licence, passport or two different utility bills that display your name and address)
- As much detail as possible regarding your request so that we can identify any information we may hold about you, this may need to include your previous name and address, date of birth and what the Superior Healthcare Group services you received.

14. Contact us

If you have any questions regarding this notice, wish to contact our Data Protection Officer, or wish to exercise any of your rights under GDPR, please contact us at the address below.

Jo Rychlik, Head of HR
Superior Healthcare Group Ltd
Gazette House
5 8 Estuary View Business Park
Boorman Way
Whitstable
Kent
CT5 3SE

Email: jorychlik@superiorhealthcare.co.uk
Tel: 1227 771133

We will always do our best to assist you to exercise your rights and give you any information you request and have the right to receive. However, if you ever feel you need to pursue a data privacy complaint further, you have the right to make a complaint to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

The contact details of the ICO are as follows:

- Helpline: 0303 123 1113
- Website: https://ico.org.uk/concerns/

Confirmation

I can confirm that I have read and received a copy of the Superior Healthcare Group's Privacy and Fair Processing Notice

Name (in PRINT): ……..

Signature: ……..

Date: ……..

(copy of this signed confirmation is to be kept on personnel file)