Privacy Notice – Employees

Last Updated: 26 February 2026
Next Review: 01 February 2027

This Privacy Notice applies to Employees, workers, bank staff, contractors, agency staff, volunteers, apprentices and applicants offered roles with Superior Healthcare Group Ltd and its operating companies (together, Superior Healthcare, we, us).

1. What information do we collect?

We collect and process personal data relating to our employees to manage the employment relationship. We are committed to being transparent about how we collect and use that data and to meeting our data protection obligations.

We collect and process a range of information about you. This includes:

- your name, address and contact details, including email address and telephone number, date of birth and gender;
- copies/scans of employment documents and personnel records (for example right to work, DBS evidence, training certificates, supervision/competency records and correspondence), where relevant to your role.
- the terms and conditions of your employment;
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the Company;
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover;
- details of your bank account and national insurance number;
- information about your marital status, next of kin, dependants and emergency contacts;
- information about your nationality and entitlement to work in the UK;
- information about your criminal record;
- details of your schedule (days of work and working hours) and attendance at work;
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave;
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence;
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence;
- information about medical or health conditions, including whether or not you have a disability for which the Company needs to make reasonable adjustments;
- details of trade union membership; and
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.

We collect this information in a variety of ways, such as:

- application forms, CVs or resumes;
- copies of your passport other identity documents;
- information collected through interviews or other forms of assessment;
- forms completed by you at the start of or during employment;
- this may also include information you enter into digital systems and forms used to deliver and record care (for example, secure online daily care log forms). This can include your name/user ID, time and date stamps, and the content of records you submit as part of your role.
- from correspondence with you;
- through meetings or other assessments;
- CCTV image footage for security purpose.

The Company will also collect personal data about you from third parties, such as:

- References supplied by former employers;
- Information from employment background check providers and information from criminal records

checks.

The Company may seek information from third parties only once a job offer to you has been made and will inform you that it is doing so.

2. How do we store your data?

Data will be stored in a range of different places, including:

- Your application record on Recruitment System – Salesforce,
- HR and Payroll management systems: Access People Planner, Access Learning and Sage.
- IT systems (including email, internal folders, Microsoft package programmes, Microsoft 365 services used for operational record keeping and collaboration, for example Microsoft Forms, SharePoint/OneDrive and Outlook shared mailboxes), where appropriate for the purpose.
- Electronic personnel files and HR records stored within our secure Microsoft 365 environment (for example SharePoint/OneDrive/secure shared drives and controlled mailboxes) with access restricted to authorised employees only, based on role and business need.
- We apply technical and organisational controls such as role-based access, multi factor authentication, audit logging, encryption and secure configuration.
- Where paper records exist (for example historic files or original documents received), they are stored securely, access is restricted, and they are digitised and/or securely destroyed in line with our retention arrangements.

3. Legislation requirements on information processing

We will only process your personal information where we are able to do so by law, under the legal basis available through the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018

The legal bases we use most often to collect information are:

- entering into and managing our employment contract
- legal obligations where processing is necessary for compliance, for example, informing HMRC of your tax and National Insurance contributions
- where the Company may rely on its legitimate interests, where a formal assessment has been made and recorded.

4. Special Category Data

Where we process sensitive personal or special categories of data about you, we will ensure this is done only where one of the following conditions applies:

- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller, or the data subject, in the field of employment and social security and social protection law;
- there is a legal obligation to process the information, where it is necessary in the public interest;
- processing is necessary for the purposes of preventive or occupational medicine, assessment of the working capacity of the employee, or the provision of health or social care;
- where it is needed in relation to legal claims.

Examples of how and when we would process the special category data:

- 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.

5. Consent

We do not normally rely on consent to process employee information, because we generally need to process it to manage the employment relationship and meet legal obligations. Where we do ask for consent (for example, for a non-essential use of your image), you can withdraw it at any time.

6. Why do we process personal data?

We need to process data to enter into an employment contract with you and to meet its obligations under your employment contract. It needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit, pension and insurance entitlements.

In some cases, the Company needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled. It is necessary to carry out criminal records checks to ensure that individuals are permitted to undertake the role in question.

In other cases, the Company has a legitimate interest in processing personal data before, during and after the end of the employment relationship.

Processing employee data allows us to:

- run recruitment and promotion processes;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;
- operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled;
- obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled;
- operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the Company complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled;
- ensure effective general HR and business administration;
- provide references on request for current or former employees;
- respond to and defend against legal claims; and
- maintain and promote equality in the workplace.

Where the Company relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

7. Who will have access to your data?

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 team if access to the data is necessary for performance of your role. Access is granted on a need-to-know basis and reviewed periodically.

Where you are involved in providing care to a client, some information you record (for example daily care logs) may be shared with the client, their authorised representative, and relevant external professionals involved in the care package (such as a case manager/commissioner), where necessary for care delivery, oversight, safeguarding, quality assurance or agreed reporting. We aim to share only what is necessary and we apply controls to reduce risk.

The Company shares your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal

records checks from the Disclosure and Barring Service.

The Company may also share your data with third parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

The Company also shares your data with third parties that process data on its behalf, in connection with payroll, the provision of benefits and the provision of occupational health services.

We may also share your data with our clients and customers, to demonstrate that all the required compliance and pre-employment checks have been completed and that you have received all the mandatory training and have the right skills to perform your role.

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

8. How does the Company protect data?

The Company takes the security of your data seriously. Internal policies and controls are in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties. Access to electronic personnel records is restricted to authorised roles, and we use audit logging to help detect and investigate any inappropriate access.

Where the Company engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and practice measures to ensure the security of data.

9. For how long does the Company keep data?

The Company will hold your personal data for the duration of your employment. The periods for which your data is held after the end of employment are set out relevant retention periods.

Employee/ worker documentation will ordinarily be retained for **seven years** after termination of employment and then promptly deleted once that period has passed. For unsuccessful job applications, documentation is retained for up to two years and then deleted.

Where records are held electronically, we apply the same retention rules and delete/securely destroy records at the end of the retention period, including any duplicate copies held in email or shared locations.

10. Keeping your data secure

We use layered security: role based access, multi factor authentication on key systems, encryption of devices, secure configuration and patching, employee training, confidentiality agreements, DPIAs for high risk processing, and incident/breach response procedures. We complete the NHS Data Security and Protection Toolkit (DSPT) annually and expect our processors to meet equivalent standards. Where paper records exist, they are stored securely and destroyed via an approved confidential waste provider (Restore). Electronic records are protected through role-based access, encryption, multi factor authentication, audit logging, and controlled sharing.

11. Your rights

As a data subject, you have a number of rights. You can:

- access and obtain a copy of your data on request;
- require the Company to change incorrect or incomplete data;
- require the Company to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- object to the processing of your data where the Company is relying on its legitimate interests as the legal ground for processing; and
- ask the Company to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the Company's legitimate grounds for processing data.

If you would like to exercise any of these rights, including when you wish to make a subject access request, please contact HR at hr@superiorhealthcare.co.uk or email dpo@superiorhealthcare.co.uk.

If you believe that the Company has not complied with your data protection rights, you can complain to the Information Commissioner (Details in Section 13).

12. What if you do not provide personal data?

You have some obligations under your employment contract to provide the Company with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith.
You may also have to provide the Company with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the Company to enter a contract of employment with you. If you do not provide other information, this will hinder the Company's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

13. Automated decision-making

Employment decisions are not based on automated decision-making.

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 the data protection legislation, please contact us at

- DPO, Superior Healthcare Group, Gazette House, 5-8 Estuary View Business Park, Boorman Way, Whitstable, Kent, CT5 3SE; or
- Email: dpo@superiorhealthcare.co.uk

We will always do our best to assist you and give you any information you request and have the right to receive. However, should you feel we have not dealt with your query to your satisfaction , you have the right to make a complaint to the **Information Commissioner's Office (ICO)**, that can be contacted on **0303 123 1113** or via www.ico.org.uk

Declaration

I can confirm that I have read and understood the Superior Group's Privacy Notice

Name (in PRINT): …….

Signature: …….

Date: …….