Employee Privacy Statement

Derbyshire Support and Facilities Services, as a data controller, collects and processes personal data relating to its 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. Any personal data shall be processed fairly and lawfully. It will only be obtained for adequate and relevant purposes and will not be kept for longer than is necessary for that purpose.

This privacy statement (sometimes referred to as a fair processing notice) tells you how your personal data will be handled and what it is used for.

What information do we collect about you?
We collect and process a range of information about you as an employee of Derbyshire Support and Facilities Services. This includes:

- Your name, address and contact details, including email addresses, phone numbers, date of birth and gender;
- The terms and conditions of your employment
- Details of your professional registration, qualifications, skills, experience and employment history, including start and end dates with previous employers and with the organisation;
- Information about your pay including entitlements to benefits such as pensions;
- Details of your bank account and national insurance number;
- Information about your marital status, next of kin, dependents and emergency contacts;
- Information about your nationality and entitlement to work in the UK;
- Information about any criminal record, if relevant;
- Details of you job plan and attendance at work;
- Details of your rotas;
- Details of periods of leave taken by you, including holiday, sickness absence, special leave and career breaks and the reasons for the leave;
- Details of any employee relations procedures in which you have been involved;
- Appraisal information and any training (including essential training) that you have participated in;
- Information about declared medical or health related conditions, including whether or not you have a disability for which the Trust needs to make reasonable adjustments;
- Details of any trade union membership; and
- Personal demographics monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.

How do we collect this information?
We collect this information in a variety of ways through telephone, email, internet and by post. Data is collected through application forms when you apply for a job with us; through our right to work and identity checks in our recruitment process i.e. from your passport or other identity documents; from forms you complete when you start work with us or during your employment with us (such as a new starter form); correspondence with you, or through interviews and meetings.

In some cases, we collect information from third parties such as references supplied by former employers and information from criminal records checks permitted by law.

Why do we need this information?
We need to process data to enter into an employment contract with you and to meet our obligations under your contract of employment. For example, we need to process your data to provide you with an employment contract, to pay you in accordance with your contract of employment and to administer benefits to you such as your pension.

In some cases, we need to process data to ensure we are complying with our legal obligations. For example, we are required to check an employee's right 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. For certain positions it is necessary to carry out criminal records checks to ensure individuals are permitted to undertake certain roles.

In other cases, we have 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 processes;
- Maintain accurate and up to date employment records and contact details (including emergency contact details), and records of employee contractual and statutory rights;
- Obtain occupational health advice, to ensure employees are receiving the support they require to carry out their role to the best of their ability.
- Operate and keep a record of other types of leave (including maternity, paternity, adoption, parental, shared parental, study and annual leave), to allow effective workforce management, to ensure that we comply with our obligations in relation to leave entitlement, and to ensure that employees are receiving the pay and benefits to which they are entitled;
- Operate and keep a record of flexible working requests to support our teams to maintain work/life balance;
- Operate and keep a record of the reasons an employee is leaving the Trust through our exit interview process to support our retention strategy;
- Operate our e-expenses system;
- Operate our staff recognition scheme;
- Operate our staff survey process;
- Comply with our obligations to provide information for regulatory purposes such as in the prevention and detection of crime and fraud;
- Operate our constitution as a public sector organisation;
- Maintain accurate and up to date training records;
- Operate our rota management system;
- Operate and keep a record of any employee relations processes;
- Meet any legal obligations under employment law;
- Ensure effective general HR and business administration;
- Provide references on request for current and former employees;
- Respond to and defend against legal claims;
- Maintain and promote equality in the workplace;

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes). Where we process other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring.

How do we store your data?

Data is stored securely in a range of different places, including in your personnel file, in our HR/payroll system and in other IT systems (including in our email system.)

Who has access to data?

Your information will be shared internally, including with members of the Workforce and Organisational Development team, of Chesterfield Royal Hospital members of the Finance Team (including payroll), your line manager, managers in the Division in which you work, members of the Corporate Governance team, members of the Internal Audit team and IT staff if access to the data is necessary for performance of their roles.

We share your data with third parties in order to obtain pre-employment references from other employers, obtain necessary criminal records checks from the Disclosure and Barring Service and manage our legal obligations.

We also share your data with third parties that process data on our behalf in connection with payroll, the provision of benefits, the provision of occupational health services and for rota management purposes. We may also share your data in order to manage our staff survey processes and to meet our regulatory obligations.

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

How do we protect your data?
We take the security of your data seriously. We have internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

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

How long do we keep data?
We will retain your information in line with the Department of Health Retention Schedule. Click here for more information.

Your rights
As a data subject, you can:

- Access and obtain a copy of your data on request;
- Require us to change incorrect or incomplete data;
- Require us 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 we are relying on its legitimate interests as the legal ground for processing; and
- Ask us to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the organisation's legitimate grounds for processing data.

Raising a concern
If you have any concerns about how your data is being processed please contact your line manager or HR Team in the first instance.

Additionally, you have the right to contact Chesterfield Royal Hospital NHS Foundation Trust's Data Protection Officer or the Information Commissioner if you should ever be dissatisfied with the way the Trust has handled or shared your personal information. Contact details are as follows:

Data Protection Officer
Chesterfield Royal Hospital NHS Foundation Trust
ICT Corridor
Calow
Chesterfield
S44 5BL
or e-mail CRHFT.DPO@nhs.net

The Information Commissioner's Office (ICO)
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113 or 01625 545745
www.ico.org.uk