Employee Privacy Statement

What is the purpose of this document?

Derbyshire Support and Facilities Services (DSFS) is committed to protecting the privacy and security of your personal information. This privacy statement describes how we collect and use personal information about you during and after your working relationship with us, in accordance with data protection law, including the UK General Data Protection Regulation (GDPR).

DSFS is a 'data controller', which means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This statement applies to current and former employees. This statement does not form part of any contract of employment or other contract to provide services, and it can be updated at any time. We will inform you if this occurs.

Data protection principles

We will comply with data protection law, which says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

What information do we collect about you?

As an employee of Derbyshire Support and Facilities Services, we collect and process a range of personal information about you. Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). There are also "special categories" of more sensitive personal data which require a higher level of protection.

The personal data we collect about you includes:

- Your name, address and contact details, including email addresses, phone numbers, date of birth, sex 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;

- Details of you job plan, workplace location 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;
- Compensation history;
- Performance and appraisal information including any training (including essential training) that you have participated in;
- Information about your use of our information and communications systems;
- CCTV footage and other information obtained through electronic means such as swipe card records;
- Photographs and videos.

We also collect, store and use the following 'special categories' of more sensitive personal information:

- Personal demographics monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief;
- Details of any trade union membership;
- Information about declared medical or health related conditions, including whether or not you have a disability for which DSFS needs to make reasonable adjustments;
- Information about accidents/injuries at work and third party accident information;
- Information about criminal convictions/allegations and offences, if relevant.

How do we collect this information?

We collect this information in a variety of ways through telephone, email, internet, electronic/information systems, physical records and by post. When you apply for a job with DSFS, your data is collected through application forms, through our right to work and identity checks in our recruitment process (i.e. from your passport or other identity documents), and through our correspondence with you, interviews and meetings. We will sometimes 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;
- Provide staff with access to wellbeing services;
- Comply with our obligations to provide information for regulatory purposes such as in the prevention and detection of crime and fraud;
- Monitor your business and personal use of our information and communication systems to ensure compliance with our IT policies;
- Ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution;
- 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;
- Deal with Freedom of Information Act requests and Subject Access Requests;
- Provide references on request for current and former employees;
- Respond to and defend against legal claims;
- Maintain and promote equality in the workplace;
- Ensure appropriate business planning and make informed decisions aimed at enhancing organisation efficiency, productivity, and overall performance.

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 ensure lawful processing?

Under the UK General Data Protection Regulations (UK GDPR), all organisations must ensure they have a clear legal basis for processing information. We will only use your personal information when the law allows us to. Most commonly, we rely on the following lawful bases to process your personal information:

Article 6(1)b of the UK GDPR; where it is necessary for performing the contract we have entered into with you.

Article 6(1)c of the UK GDPR; where we need to comply with a legal obligation.

Article 6(1)f of the UK GDPR; where it is necessary to process your data but not in connection with the performance of a contract or compliance with a legal obligation.

When processing your personal information, which classifies as 'special category data', we rely on the following lawful bases:

Article 9(1)b of the UK GDPR; where it is necessary to process your personal data for things directly related to your employment contract(s), such as payroll, benefits administration or tax purposes.

Article 9(1)f of the UK GDPR; where processing is necessary for the establishment, exercise or defence of legal claims.

There can be rare occasions where it becomes necessary to use your personal information to protect your vital interests (or someone else's). In such instances, we rely on Article 6(1)d and Article 9(1)c of the UK GDPR.

Do we rely on your consent?

We do not rely on your consent when we use your personal information for the purposes depicted in this statement. We also do not tend to rely on consent in any other data processing activities due the clear imbalance of power between yourself, as the Data Subject, and DSFS, as the data controller.

How do we store your personal information?

Data is stored securely in a range of different places, including in your personnel file, our HR/payroll system and other IT systems (including our email system). We ensure that all the IT systems we utilise undergo thorough assessments in relation to data protection and security to uphold the confidentiality and integrity of your personal information.

Who do we share your personal information with?

Your information will be shared internally with staff and departments responsible for abovementioned data processing activities. As a subsidiary wholly owned by Chesterfield Royal Hospital NHS Foundation Trust, we will share your data with relevant staff and departments such as the Workforce and Organisational Development Team to support the management of your employment and related administrative tasks.

We share your data with third parties, who provide software and services to facilitate the abovementioned data processing activities, and to obtain pre-employment references from other employers, obtain necessary criminal records checks from the Disclosure and Barring Service and manage our legal obligations. Additionally, we may use sub-processors to support our business planning activities such as conducting data analytics studies to review and better understand employee retention and attrition rates. When sharing your data with external parties, we make sure that applicable data protection laws are adhered to and appropriate safeguards to protect your privacy are in place.

What happens if you don’t provide personal information?

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

Please note that we will if necessary process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

For how long do we keep your personal information?

Retention periods differ based on the type of personal information. Generally, we store your data in line with the following legislation:

- Data Protection Act 2018
- Fire Precautions (Workplace) Regulations 1997
- Former statutory guidance 'Claim for wages through the Coronavirus Job Retention Scheme'
- Health and Safety (Consultation) Regulations 1996
- Health and Safety (First Aid) Regulations 1981
- Health and Safety Information for Employees Regulations 1989
- HMRC VAT deferral guidance
- Limitation Act 1980
- National Minimum Wage Act 1998 and The National Minimum Wage (Amendment) Regulations 2021
- Public Interest Disclosure Act 1998 and recommended IAPP practice
- Taxes Management Act 1970
- The Companies Acts 2006
- The Control of Asbestos at Work Regulations 2012
- The Control of Lead at Work Regulations 2002
- The Control of Substances Hazardous to Health Regulations 2002
- The Income Tax (Employments) Regulations 1993
- The Ionising Radiations Regulations 1999
- The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995
- The Retirement Benefits Schemes (Information Powers) Regulations 1995
- The Statutory Maternity Pay (General) Regulations 1986 as amended, Maternity & Parental Leave Regulations 1999
- The Working Time Regulations 1998 (SI 1998/1833) and Employment Rights Regulations 2023

How do we protect your data?

We take the security of your data seriously. We have internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by 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 organisation measures to ensure the security of your data.

Your rights as a Data Subject

Under certain circumstances you have the right to:

- **Request access** to your personal information (commonly known as the 'data subject access request'). This enable 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 information that we hold about you. This enables you 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 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).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground.
- **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.
- **Receive personal data** you have provided to us in a structured, commonly used and machine readable format.

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, please contact crhft.dsfshumanresources@nhs.net in writing.

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we are allowed under the law to charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we can refuse to comply with the request in such circumstances.

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

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, DSFS have appointed a Data Protection Officer (DPO) to oversee compliance with this privacy notice. Contact details are as follows:

Data Protection Officer
Chesterfield Royal Hospital NHS Foundation Trust
ICT Corridor
Calow
Chesterfield
S44 5BL

Or email crhft.dpo@nhs.net

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

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

Changes to this privacy statement

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates.

Document version: 2.0
Fist published: 01/12/2018
Last update: 10/10/2025