

Staff Privacy Notice

The information that we collect

This Privacy Notice explains what personal information we collect from you, how we store this personal information, how long we retain it and with whom and for which legal purpose we may share it. During the course of your employment, Sheffield Teaching Hospitals NHS Foundation Trust collects, stores and processes personal information about prospective, current and former staff. This Privacy Notice includes applicants, employees (and former employees), workers (including agency, casual and contracted staff), volunteers, trainees and those carrying out work experience. We recognise the need to treat staff personal and sensitive data in a fair and lawful manner. No personal information held by us will be processed unless the requirements for fair and lawful processing can be met.

We are required by law to provide you with the information in the following subsections:

<p>Who we are (Data Controller)</p>	<p>Sheffield Teaching Hospitals NHS Foundation Trust provides a full range of hospital and community services for people in Sheffield, as well as specialist care for patients from further afield.</p> <p>The Trust is registered with the Information Commissioner’s Office to process personal and special categories of information under the Data Protection Act 2018 and our registration number is Z8751481.</p> <p>Our address is:</p> <p>Sheffield Teaching Hospital NHS Foundation Trust Department of Information Governance, Caldicott and SIRO Support Royal Hallamshire Hospital 2 Claremont Place Sheffield S10 2TB</p>
<p>Data Protection Officer</p>	<p>Data Protection Officer Department of Information Governance, Caldicott and SIRO Support Royal Hallamshire Hospital 2 Claremont Place Sheffield S10 2TB</p> <p>Telephone: 0114 2265151 Email: sth.infogov@nhs.net</p>



<p>Why we collect and how we use your personal information</p>	<p>The Trust collects, stores and processes personal information about prospective, current and former staff to ensure compliance with legal or industry standards such as:</p> <ul style="list-style-type: none"> • Employment and employment-related law: as applicable to circumstances, including occupational health, pensions, provision of IT services and equipment, health and safety, etc. • Obligations in relation to the provision of health services (examples: incident reporting and investigation, staff names in patient records). • Obligations in relation to registered professions as provided by registration bodies, or other legislation (examples: Duty of Candour; transparency obligations in relation to declarations of interest, freedom of information, etc.)
<p>Lawful basis for processing</p>	<p>The Trust only processes your personal data where we have your consent or where the processing can be legally justified. These include circumstances where the processing is necessary for the performance of staff contracts with us or for compliance with any legal obligations, which applies to the Trust as your employer; this will include sharing your information with other bodies where we have a statutory or legal obligation to do so.</p> <p>The Trust's legal basis for processing staff information are defined on:</p> <ul style="list-style-type: none"> • 6(1)(c) necessary for legal obligations. • 9(2)(b) employment provisions (see also Article 88). • 9(2)(c) processing for 'vital interests' (safety, safeguarding, public safety, etc.) • 9(2)(h) occupational health provisions.
<p>What personal information do we need to collect about you and how do we obtain it?</p>	<p>Personal information about you will largely be collected directly from you during your recruitment and employment. Your information could be collected in a number of different ways. This could be directly from you, in person, over the telephone or on a form you have completed, such as a job application, contractual documentation or time-sheet. Personal information may also be collected from healthcare professionals in certain circumstances, through national checks such as the Disclosure and Barring Service (DBS). Details might also come from other external sources such as NHS jobs, your professional body, current or previous employers or government bodies like HM Revenue and Customs, the Department for Work and Pensions or the UK Visas and Immigration.</p> <p>In order to carry out our activities and obligations as an employer we handle data in relation to:</p> <ul style="list-style-type: none"> • Personal demographics (including gender, race, ethnicity, sexual orientation, religion)



	<ul style="list-style-type: none"> • Contact details such as names, addresses, telephone numbers and emergency contact(s) • Employment records (including professional membership, references and proof of eligibility to work in the UK and security checks) • Bank details • Pension details • Occupational health information (medical information including physical health or mental condition) • Information relating to health and safety • Trust’s governors / membership • Offences (including alleged offences), criminal proceedings, outcomes and sentences • Information relating to employee relations, including disciplinary proceedings, grievances and complaints and tribunal claims <p>Our staff are trained to handle your information correctly and protect your confidentiality and privacy. We aim to maintain high standards, adopt best practice for our record keeping and regularly check and report on how we are doing. Your information is never collected or sold for direct marketing purposes.</p>
<p>Who we share your personal information with</p>	<p>We will only share your information with other bodies where we have a statutory or legal obligation to do so. These obligations may include (but are not limited to):</p> <ul style="list-style-type: none"> • Staff administration and management (including payroll and performance) • Pension administration • Business management and planning • Accounting and Auditing • Accounts and records • Education, training and development • Health administration and services • Information and database administration • Criminal prosecution and prevention • National fraud initiatives • Quality monitoring, including, for example, staff surveys • Used for the modelling the future provision and configuration of health and social care within Sheffield <p>Where possible, we will always look to anonymise / pseudonymise your personal information so as to protect confidentiality, unless there is a legal basis that permits us to use it, and we will only use it, and will only ever use / share the minimum information necessary. However, there are occasions where the Trust is required by law to share the information provided to us with other bodies responsible for auditing or administering public funds, in order to prevent and detect fraud. Any disclosures of personal data are always made on a case-by-case basis, using the minimum personal data necessary for the specific purpose and circumstances and with the</p>



	<p>appropriate security controls in place.</p> <p>For any request to transfer your data internationally outside of the UK/EU we will make sure that an adequate level of protection can be satisfied before the transfer.</p> <p>There are a number of circumstances where we must or can share information about you to comply or manage with:</p> <ul style="list-style-type: none"> • Disciplinary / investigation processes; including referrals to Professional Bodies, e.g. NMC and GMC • Legislative and / or statutory requirements • A Court Order which may have been imposed on us • NHS Counter Fraud requirements • Request for information from the Police and other law enforcement agencies for the prevention and detection of crime and / or fraud if the crime is of a serious nature. <p>You have the right to refuse (or withdraw) consent to information sharing at any time. However, this may not be possible if the sharing is a mandatory or legal requirement imposed on the Trust. Any restrictions, and the possible consequences of withholding your consent, will be fully explained to you as the situation arises.</p>
<p>How long do we retain your information?</p>	<p>Your data will be retained in line with the NHS Records Management Code of Practice – Retention Schedule.</p> <p>Records Management Code of Practice 2020 - NHSX</p> <p>Or contact the Trust Data Protection Officer should you require further details.</p>
<p>What are your rights?</p>	<p>If we need to use your information for any reasons beyond those stated in this Privacy Notice, we will discuss this with you and ask for your explicit consent. The General Data Protection Regulation and the Data Protection Act 2018 gives you certain rights, including the right to:</p> <ul style="list-style-type: none"> • Request to access the personal data we hold about you, e.g. personnel records. • Request the correction of inaccurate or incomplete information recorded in our records, subject to certain safeguards. • Request that your information be deleted or removed where there is no need for us to continue processing it and where the retention time has passed. • Ask us to restrict the use of your information where appropriate. • Ask us to copy or transfer your information from one IT system to another in a safe and secure way, without impacting the quality of the information. • To object to how your information is used.



	<ul style="list-style-type: none"> To challenge any decisions made without human intervention (automated decision making).
<p>How can you contact us with queries or concerns about this privacy notice?</p>	<p>If you have any queries or concerns regarding the information that we hold about you or you have a question regarding this Privacy Notice, please contact our Information Governance team:</p> <p>Information Governance Department 2 Claremont Place Sheffield S10 2TB</p> <p>Telephone: 0114 2265153 E-mail: sth.infogov@nhs.net</p>
<p>How can you make a complaint?</p>	<p>You have the right to make a complaint if you feel unhappy about how we hold, use or share your information. Depending on the nature of your complaint, we would recommend contacting your line manager in the first instance.</p> <p>Alternatively, you can contact our Information Governance team (contact details, provided above) who will help you to identify the most appropriate procedure to follow based on the specifics of your complaint.</p> <p>If you remain dissatisfied following the outcome of your complaint, you may wish to contact the Information Commissioner’s Office (ICO). The ICO is the body that regulates the Trust under Data Protection and Freedom of Information legislation. Contact details for the ICO are as follows:</p> <p>Information Commissioner’s Office Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF</p> <p>e-mail: https://ico.org.uk/global/contact-us/</p> <p>Tel: 0303 123 1113 (local rate) or 01625 545 745 (national rate)</p> <p>Please note that the Information Commissioner will not normally consider an appeal until you have exhausted your rights of complaint to us directly. Please see the ICO website for further advice / details.</p>
<p>National Fraud Initiative Fair Processing Notice</p>	<p>The Trust is required [by law] to protect the public funds it administers. It may share information provided to it with other bodies responsible for; auditing, or administering public funds, or where undertaking a public function, in order to prevent and detect fraud.</p> <p>The Cabinet Office is responsible for carrying out data matching exercises. Data matching involves comparing computer records held by one body against other computer records held by the same or another body to see how far they match. This is usually personal information. Computerised data</p>



matching allows potentially fraudulent claims and payments to be identified. Where a match is found it may indicate that there is an inconsistency which requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out.

We participate in the Cabinet Office’s National Fraud Initiative: a data matching exercise to assist in the prevention and detection of fraud. We are required to provide particular sets of data to the Minister for the Cabinet Office for matching for each exercise, as detailed here.

The use of data by the Cabinet Office in a data matching exercise is carried out with statutory authority under Part 6 of the Local Audit and Accountability Act 2014. It does not require the consent of the individuals concerned under the Data Protection Act 2018.

Data matching by the Cabinet Office is subject to a Code of Practice. View further information on the Cabinet Office’s legal powers and the reasons why it matches particular information.

For further information on data matching at this organisation please contact Claire Croft on 01709 428710.

Document Control

Version	5
Document Lead	Michael Maginnis, Head of Information Governance/Data Protection Officer
Approval body	Information Governance Group
Date approved	16 September 2024
Issue date	30 September 2024
Review Date	16 September 2027

