

Trust Staff Information Privacy Notice

Everyone working for the Trust has a legal duty to keep personal information confidential, which includes that of staff members

This Privacy Notice describes how the Trust uses and processes the information it holds about all employees of the Trust. It includes (but not limited to) agency, contract and temporary staff, volunteers and students in support of the Trust, including how the information may be shared with other organisations, and how the confidentiality of information is maintained.

South Tees Hospitals NHS Foundation Trust is registered with the Information Commissioner's Office (ICO) as a data controller and collects data for a variety of purposes. The Trust Registration Number is: **Z5832686**

For the purposes of this Privacy Notice "staff" includes all employees, including but not limited to, permanent staff, agency, contract and temporary staff, volunteers and students.

Data Protection Principles

We will comply with data protection law. This 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.

How is information about me used by the Trust?

The Trust collects and uses your information for the lawful purposes of administering the business of the Trust and carrying out its obligations in relation to employment.

As an employee, the Trust does not need to obtain your consent to process your information, these purposes include:

- Management and development of the Trust workforce including staff retention;
- Monitoring and management of occupational health;
- To allow better financial modeling and planning;
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process)
- Specialist categories of data, to include;
 - Trade Union Membership

- To retain Biometric information to enable access to Trust systems
- Information about your health, including any medical conditions, health and sickness records
- For the purposes of monitoring – Race, Ethnic origin, Religion, Sexual orientation, Disability and other protected characteristics
- To keep images that appear in Trust or other publications or websites to market and promote the Trust;
- To allow the Trust policies to be implemented and acted upon when appropriate.
- Administration of staff parking, access control (including ID badges), switchboard facilities and staff residences.

There are many reasons linked to staff administration of your employment such as paying you and processing any changes that happen as a result of your career development.

Information about you is specifically processed under Articles 6(1)(b) and 9(2)(h) of the General Data Protection Regulation 2016

What information is collected about me?

In order to carry out our activities and obligations as an employer we handle information about you in relation to:

- Personal details such as name, address, telephone number(s), date of birth.
- Personal demographics (including gender, race, ethnicity, sexual orientation, religion)
- Medical information (including physical and/or mental health)
- Emergency contact(s), eg next of kin details
- Education and training
- Employment details (including job role, place of work, references and proof of eligibility to work in the UK)
- Attendance records including holidays, periods of absence etc.
- Membership of professional bodies and/or trade union(s)
- Bank details, eg in order to pay your salary
- Pension details
- Offences (including alleged offences), criminal proceedings, outcomes and sentences
- Information pertinent to employee relation matters.
- Employment tribunal applications, complaints, accidents and incident details
- Visual images, eg photographs on staff notice boards or CCTV monitoring
- Supervision and appraisal documentation
- Sickness absence and annual leave details
- Complying with Health & Safety, and Safeguarding obligations
- To prevent fraud, bribery or corruption
- Administering the employment contract with trust employees

The Trust only collects information about criminal convictions if it is appropriate given the nature of the role and where we are legally required to do so. Where appropriate, the Trust will collect information about criminal convictions as part of the recruitment process, or we may be notified of such information directly by you, or by appropriate regulating authorities. The Trust is permitted to use your personal information in this

way to undertake obligations to comply with the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (Amendment) (England and Wales) 2013.

There is an appropriate policy and safeguards in place as required by law to maintain such data.

You should be aware that once you have approved your image ie photograph, video etc to appear in a publication (usually done verbally) we may not be able to completely retrieve this image if you change your mind about its use. Your image may appear again at a later date unless you specifically indicate otherwise.

The Trust may use your information in order to gather evidence for disciplinary and other staff processes. The use of this information will always be proportionate in relation to the evidence being sought.

Lateral Flow Testing

What happens to my personal information after I submit my test results?

The Trust is required by the Department of Health and Social Care, Public Health England and as part of the national NHS Test and Trace programme to provide the details of staff tests undertaken. This fulfils the statutory reporting requirements for COVID-19 testing. Information that will be provided includes; your full name, gender, date of birth, address, email address, mobile phone number date of your test and test result. The sharing of this data is covered under the Control of Patient Information regulation (<https://digital.nhs.uk/coronavirus/coronavirus-covid-19-response-information-governance-hub/control-of-patient-information-copi-notice>) and your data will be handled in strict confidence. For further information and to view a copy of the national privacy notice please visit this link: <https://www.gov.uk/government/publications/coronavirus-covid-19-testing-privacy-information/testing-for-coronavirus-privacy-information--2>

Flu vaccines and the COVID-19 response

On average, flu kills over 11,000 people each year – some years this number is much higher – and it hospitalises many more. This is anything but a typical year due to the potential impact of flu and COVID-19 circulating at the same time.

This year, as well as GP practices inviting key eligible groups to receive their vaccination, reminders have gone out nationally to supplement this. COVID-19 vaccines will also be managed centrally once they are available. Given the potential time gap required between the flu and COVID-19 vaccines, it is important that the invites, reminders and uptake of the vaccines are carefully managed together and regarded as part of the response to the COVID-19 pandemic.

This guidance describes how data is being used to help ensure that those who are entitled to a flu vaccine receive one. This includes data relating to both health and care staff and patients.

For full details please see link below:

<https://www.nhs.uk/information-governance/guidance/flu-vaccines-and-covid-19-response/>

Streamlining

Streamlining is the process by which certain personal data is available and can be transferred from one NHS organisation to another when your employment transfers within the NHS. NHS organisations have a legitimate interest in processing your data in this way in ensuring the employment of a suitable workforce.

In accepting employment with the Trust, you accept that the following personal data will be transferred under the streamlining programme if your employment transfers to another NHS organisation:

- Training records
- Immunisation and vaccination records
- Personal data such as name, address, date of birth, national insurance number
- Relationship data such as next of kin, doctor and dependents
- Current Sickness absence record over previous two years
- Employment dates, job title and grades
- Current disciplinary action or ongoing investigations or safeguard referrals
- Disclosure & Barring Service (DBS) check information with date and level

The ESR streamlining programme is a data sharing arrangement designed to improve efficiencies in the NHS both to make costs savings for Trust but also to save you time when your employment transfers within the NHS.

The Trust remains as the data controller for the purposes of GDPR/Data Protection and ESR is the data processor. When your personal data is transferred, the recipient NHS organisation becomes the data controller of your personal data.

In order to carry out our activities and obligations as an employer we handle information about you in relation to:

- Personal details such as name, address, telephone number(s), date of birth.
- Personal demographics (including gender, race, ethnicity, sexual orientation, religion)
- Medical information (including physical and/or mental health)
- Emergency contact(s), e.g. next of kin details
- Education and training
- Employment details (including job role, place of work, references and proof of eligibility to work in the UK)
- Membership of professional bodies and/or trade union(s)
- Bank details, e.g. in order to pay your salary
- Pension details
- Offences (including alleged offences), criminal proceedings, outcomes and sentences
- Employment tribunal applications, complaints, accidents and incident details
- Visual images, e.g. photographs on staff notice boards or CCTV monitoring
- Supervision and appraisal documentation

- Sickness absence and annual leave details

How is Information kept about me?

Your information is stored in both paper (personnel files held by your line manager) and electronically on the Electronic Staff Record (ESR) system. Other temporary files may be created as a result of investigations, disciplinarys or complaints but these will usually be kept separately from the personnel file or destroyed in line with the agreed destruction criteria. If a sanction is applied, it will be noted on the personnel file.

Who do you share my information with?

We will not routinely disclose any information about you to anyone outside the Trust without your consent. However, there are circumstances where we must or can share information about you owing to a legal/statutory requirement. We may obtain and share personal information with a variety of other bodies, which may include, but is not limited to:

- Her Majesty's Revenue and Customs (HMRC)
- Department for Work and Pensions (DWP)
- Disclosure and Barring Service (DBS)
- Home Office
- Child Support Agency
- Regulatory bodies, e.g. NMC, GMC
- Law enforcement agencies including the Police and the Serious Organised Crime Agency
- NHS Counter Fraud

Cabinet Office: National Fraud Initiative (NFI)

South Tees Hospitals NHS Foundation Trust is required 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.

The Cabinet Office is responsible for carrying out data matching exercises that involves comparing sets of data such as the payroll records of a body against other records held by the same or another body to see how well they match. This 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 another explanation until an investigation is carried out.

The processing of data by the Cabinet Office in a data matching exercise is carried out with statutory authority under its powers in Part 6 of the Local Audit and Accountability Act 2014. It does not require the consent of the individuals concerned under data protection legislation or the GDPR (General Data Protection Regulation). Data matching by the Cabinet Office is subject to a code of data matching practice, also available on the www.gov.uk website.

Further information can be sought from the Counter Fraud team by telephone on: 0191 441 5936 or by email at counterfraud@audit-one.co.uk.

Third Party Service Providers

We will share your personal information with third parties where required by law or contract, or where it is necessary to administer the working relationship with you.

Third-party service providers may include contractors and designated agents which provide services such as, payroll, pension's administration, IT service etc. on behalf of the Trust and its employees.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

How long will you keep my information?

We will keep your employment information for the periods defined in the Records Management Code of Practice for Health and Social Care 2016. Specifically, we will retain your detailed information for a period of seven years after you leave the Trust's employment at which point we will create a summary of your staff record and retain this until your 75th Birthday. Your main employment record with the Trust will be destroyed seven years after you leave.

How can I access my information?

You can request access to the information that the Trust holds about you and you should do this by approaching your line manager in the first instance. They will provide you with guidance on the Trust's processes. Your request, once agreed with you, will be completed within one calendar month. However, if your records are extensive we may take longer to process your request but will inform you from the outset. Alternatively you can contact the Human Resources Team.

Information that you are entitled to:

In addition to receiving a copy of the information that the Trust holds and processes you are also entitled to the following:

- To be informed if any personal data is being processed.
- Given a description of the personal data, the reasons it is being processed, and if it will be given to any other organisations or people.
- Given a copy of the personal data together with its source (where this is available).

How do you make sure it is safe and secure?

We will use your information in a way that follows data protection laws and Trust policies and procedures.

Everyone working for the NHS is subject to the Common Law Duty of Confidence. Information provided in confidence will only be used for the purposes advised and consented to, unless it is required or permitted by the law.

All Trust staff are required to undertake mandatory Information Governance training,

which covers how personal information should be processed.

We do not transfer staff or job applicant personal information to a country outside of the European Union (EU) unless the staff member / job applicant is located outside of the EU. In such cases the Trust will ensure that all communications are conducted securely.

Staff as Foundation Trust Members

Staff automatically become members when employed by the Trust; this includes individuals who exercise functions for the purpose of the Trust otherwise under a contract of employment (provided they have a contract of employment for a period of at least 12 months). The Trust has a legal basis for carrying out this process. This means that your name and contact details will be used to provide you with relevant information relating to membership which includes details of how to nominate yourself to become a Staff Governor or how to vote in any Staff Governor elections. For this purpose we would share your details with an Election Agent who would act as the data processor for this purpose. You have the right to opt out of membership at any time by emailing the Foundation Trust Office at stees.foundation.trust@nhs.net.

Further Information

Data Protection Officer

The Trust's Data Protection Officer (DPO) is responsible for ensuring that the Trust complies with the GDPR. The DPO is the person to contact if you would like to know more about how we use your information, require information in any accessible format or language or if (for any reason) you do not wish to have your information used in any of the ways described. Their contact details are:

Steven Orley – Head of Information Governance & Data Protection Officer
South Tees Hospitals NHS Foundation Trust
The James Cook Hospital
Marton Road
Middlesbrough
TS4 3BW

Or email to stees.dpo@nhs.net

For independent advice about data protection, privacy and information-sharing issues you can contact the Information Commissioner:

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow,
Cheshire
SK9 5AF
Phone: 08456 30 60 60 or 01625 54 57 45
Website: www.ico.org.uk