Privacy Notice – Staff

This privacy notice tells you what to expect us to do with your personal data when we collect personal data about you.

Our contact details

Name:	North Staffordshire Combined Healthcare NHS Trust
Address:	Lawton House, Bellringer Road, Trentham Stoke-on-Trent ST4 8HH
General phone number:	0300 123 1535

Website: www.combined.nhs.uk

We are the controller for your data. A controller decides on why and how data is used and shared.

Data Protection Officer contact details

Our Data Protection Officer is responsible for monitoring our compliance with data protection requirements. You can contact them with queries or concerns relating to the use of your personal data at DPO@combined.nhs.uk.

How do we get your data?

We get information about you from the following sources:

- Directly from you
- From an employment agency
- From your employer if you are on secondment to NSCHT
- From referees, either external or internal
- From security clearance providers
- From Occupational Health and other health providers
- From Pension administrators and other government departments, for example tax details from HMRC
- From your Trade Union
- From providers of staff benefits
- CCTV images from our landlords or taken using our own CCTV systems

Lawful basis for processing your personal data

Depending on the processing activity, we rely on the following lawful basis for processing your personal data under current Data Protection Legislation:

- Article 6(1) (b) which relates to processing necessary for the performance of a contract
- Article 6(1) (c) so we can comply with our legal obligations as your employer
- Article 6(1) (d) in order to protect your vital interests or those of another person
- Article 6(1) (e) for the performance of our public task
- Article 6(1) (f) for the purposes of our legitimate interest

Special category data

Where the information we process is special category data, for example your health data, the additional bases for processing that we rely on are:

- Article 9(2) (b) which relates to carrying out our obligations and exercising our rights in employment and the safeguarding of your fundamental rights
- Article 9(2) (c) to protect your vital interests or those of another person where you are incapable of giving your consent
- Article 9(2) (h) for the purposes of preventative or occupational medicine and assessing your working capacity as an employee
- Article 9(2) (f) for the establishment, exercise or defence of legal claims
- Article 9(2) (j) for archiving purposes in the public interest

In addition, we rely on processing conditions at Schedule 1 part 1 paragraph 1 and Schedule 1 part 1 paragraph 2(2) (a) and (b) of the DPA 2018. These relate to the processing of special category data for employment purposes, preventative or occupational medicine and the assessment of your working capacity as an employee.

What personal data we process and why

Data related to your employment

We use the following data to carry out the contract we have with you, provide you access to business services required for your role and manage our people operations processes. We will also use it to adhere to regulatory requirements as advocated by the Care Quality Commission (CQC) whose job is to regulate activities for all health and social care organisations, as well as abide by key data protection principles as regulated by the Information Commissioners Office:

- Personal contact details such as your name, address, contact telephone numbers (landline and mobile) and personal email addresses (this could include for long service awards and staff wellbeing initiative purposes)
- Your date of birth, gender and NI number
- A copy of your passport or similar photographic identification and / or proof of address documents to ensure that you have a right to work in the UK – the Home Office can (and does) audit employers without notice and there's a £20,000 fine for each individual without proof of 'right to work' on their personal file
- Marital status
- Next of kin, emergency contacts and their contact information
- Employment and education history including your qualifications, job application and employment references, professional memberships, right to work information and details of any criminal convictions that you declare
- Location of employment (e.g., which site will be your base)
- Occupational Health Pre-Employment Assessment Outcomes to ensure fitness to work
- Details of any secondary employment, political declarations, conflict of interest declarations or gift declarations
- Security clearance details including basic checks and higher security clearance details according to your job
- Any criminal convictions that you declare to us
- Your responses to staff surveys if this data is not anonymised (The data collected from staff surveys is processed by Quality Health (unless internal). Any data collected by Quality Health for us is stored on UK servers. Most survey questions require quantitative responses; however, some free text boxes are included. We advise you not to share identifiable information about yourself in these boxes if you wish to remain anonymous. Any question returning fewer than 11 responses cannot (is not) included in results to ensure that individuals cannot be identified
- Vehicle Licence Plate details - the car park scheme at the Harplands Hospital is operated by our Estates department who will hold vehicle licence plate details linked to you. These details are deleted when members leave the scheme. For sites that do not operate a car parking scheme, staff may be asked to provide car registration details with Reception staff to aid safety provisions. Any information provided to Reception staff will be handled in the same way as any staff information, always ensuring adherence to strict confidentiality requirements.
- Vehicle details including registration number, proof of ownership, proof of MOT (if applicable) and insurance and driving licence if you will be using your car for business purposes – these will be kept in your personal file which is held by your line manager and uploaded onto EASY (expenses system).

Data related to your salary, pension and loans

We process this information for the payment of your salary, pension and other employment related benefits. We also process it for the administration of statutory and contractual leave entitlements such as holiday or parental leave. It is necessary for the execution of the employment contract and also for HMRC purposes.

We are legally obliged to retain payroll information for seven years after termination of employment for HMRC purposes.

- Data about your job role and your employment contract including your start and leave dates, salary (including grade and salary band), any changes to your employment contract, working pattern (including any requests for flexible working)
- Details of your time spent working and any overtime, expenses or other payments claimed, including details of any loans such as for travel season tickets
- Details of any leave including sick leave, holidays, special leave etc
- Pension details including membership of both state and NHS pension schemes (current and previous)
- Your bank account details, payroll records and tax status information
- Trade Union membership for the purpose of the deduction of subscriptions directly from salary
- Details relating to Maternity, Paternity, Shared Parental and Adoption leave and pay. This includes forms applying for the relevant leave, copies of MATB1 forms/matching certificates and any other relevant documentation relating to the nature of the leave you will be taking

Data relating to your performance and training

We use this data to assess your performance, to conduct pay and grading reviews and to deal with any employer / employee related disputes. We also use it to meet the training and development needs required for your role.

- Data relating to your performance at work e.g., probation reviews, 1-2-1s, PDRs, promotions
- Grievance and dignity at work matters and investigations to which you may be a party or witness
- Disciplinary records and documentation related to any investigations, hearings and warnings/penalties issued
- Whistleblowing concerns raised by you, or to which you may be a party or witness. We have policies and procedures in place to enable our current staff and ex-employees to have an avenue for raising concerns (multiple routes for this to take place: Dispute and Grievance Resolution Policy, Freedom to Speak UP, Whistleblowing) about malpractice. Information in this context is processed by us because it is necessary for our compliance with our legal obligations under the Public Interest Disclosure Act 1998 and The Public Interest Disclosure (Northern Ireland) Order 1998. Although every effort will be taken to restrict the processing of your personal data and maintain confidentiality whether this is possible will be dependent on the nature of the concern and any resulting investigation
- Data related to your training history and development needs. Our Workforce and Development and Planning department use online learning platforms such as Learning Management System (LMS) for the facilitation of its work-related courses. We also use the NHS E-learning for Health. We will share some information about you with these providers both prior to you joining us and during your employment to ensure you have the necessary access to complete training required for your role. We will also share information about you with our training providers. For example, this will include information such as your name, contact details and job role. When necessary, we will also share information about any dietary or access requirements that you might have when you attend training events to ensure reasonable adjustments are made to accommodate individual needs

Data relating to monitoring

We use this data to assess your compliance with corporate policies and procedures and to ensure the security of our premises, IT systems and employees.

- Data about your access to data held by us for the purposes of criminal enforcement if you are involved with this work
- Data derived from monitoring IT acceptable use standards
- Photos and CCTV images

All our ICT systems and the door access system for the entry and exit of our premises are auditable and can be monitored. All staff are issued with a security pass that displays their name, job title and photograph. Staff pass

details (names, job title and photographs) are held on a system controlled by our Estates Team and can only be accessed by a restricted number of people. Should you lose your pass you will need to notify the Estates Team as soon as possible and also report it to the Information Governance Team, who will ensure appropriate procedures are followed. When you leave us, your details are deleted as soon as possible from this system as part of the leaver's process.

We are committed to respecting individual users' reasonable expectations of privacy concerning the use of our ICT systems and equipment. However, we reserve the right to log and monitor such use in line with our Acceptable Use Standard.

Any targeted monitoring of staff will take place within the context of our disciplinary procedures.

We operate CCTV on and around our premises to monitor access to certain areas. Further information is available in our CCTV policy, which details how requests to view/access footage can be appropriately made. You have the right to request your data captured on CCTV.

Additionally, staff working from other sites may be filmed by CCTV which is owned and operated by the landlords or owners of the buildings in which our offices are situated. We are not the data controller for this information.

Data relating to your health and wellbeing and other special category data

We use the following data to comply with our legal obligations and for equal opportunities monitoring. We also use it to ensure the health, safety and wellbeing of our employees.

- Health and wellbeing information either declared by you or obtained from health checks, eye examinations, occupational health referrals and reports, sick leave forms, health management questionnaires or fit notes i.e., Statement of Fitness for Work from your GP or hospital. We use Optima Health to provide our occupational health service. The data you provide will be held by Optima Health
- Accident records if you have an accident at work
- Details of any desk audits, access needs(including Display Screen Equipment Assessments) or reasonable adjustments
- Data you have provided regarding Protected Characteristics as defined by the Equality Act 2010 and s.75 of the Northern Ireland Act for the purpose of equal opportunities monitoring. This includes racial or ethnic origin, religious beliefs, disability status, and gender identification and may be extended to include other protected characteristics – this information is anonymised when used for reporting purposes
- Equal opportunities information provided by job applicants is attached to the relevant application on our applicant tracking system TRAC when you apply for a role at with us. This information is not made available to any staff outside our recruitment team (including hiring managers) in a way which can identify you. This information is anonymised after six months and retained for reporting purposes only

The Trust recognised unions (Unison) are controllers for the personal information connected to your union membership. We hold some union subscription details to process salary deductions for union membership for which you will have given your consent.

Security Clearance and criminal convictions and offences

Basic security checks and / or advanced checks based on your role in line with the Baseline Personnel Security Standards and the government Security Policy Framework are carried out by HMRC on our behalf.

NSCHT security clearance applications are processed by the Disclosure and Barring Service (DBS). To ensure we remain updated on DBS status, an automated search tool links from our Electronic Staff Record (ESR) system to the DBS system to ensure any changes in an individual's staff DBS status are notified to us as the employer and remains a legitimate processing activity. These checks are run every 60 days and ensure as an employer we remain updated on any specific and pertinent changes in DBS status.

In addition, some staff are required to get Security Clearance, Developed Vetting (DV) or a Counter Terrorist Check (CTC) which is also carried out by HMRC. The outcome of these checks are stored on our systems.

We process data about staff criminal convictions and offences. The lawful basis we rely on to process this data are:

- Article 6(1) (e) for the performance of our public task. In addition, we rely on the processing condition at Schedule 1 part 2 paragraph 6(2) (a)

- Article 6(1) (b) for the performance of a contract. In addition, we rely on the processing condition at Schedule 1 part 1 paragraph 1

Retention of Personal Data

We adhere to the NHS Records Management Code of Practice for Health and Social Care and national archives requirements regarding the retention of your personal data. More information on the relevant retention periods can be found in the NHS Records Management Code of Practice 2021.

Physical and electronic records are held for each member of staff. Data is held securely across the various sites.

Who do we share data with?

In some circumstances, such as under a court order, we are legally obliged to share information. We may also share information about you with third parties including government agencies and external auditors. For example, we may share information about you with HMRC for the purpose of collecting tax and national insurance contributions.

Additionally, we are required under the Public Records Act 1958 (as amended) to transfer records to the National Archives (TNA) for permanent preservation. Some of these records may include the personal data of our current and former employees. Full consideration will be given to Data Protection and Freedom of Information legislation when making decisions about whether such records should be open to the public.

The Trust is also legally obliged to provide data to the Police or NHS Counter Fraud where there may be criminal investigations/proceedings. There are exemptions under UKGDPR to allow the Trust as an employer to disclose data under these circumstances.

Disclosures under the Freedom of Information Act

As a public authority we receive information requests under the Freedom of Information Act (2000) about our staff and we must consider whether to disclose staff information (including agency and temporary staff) in response to these requests.

We will normally disclose work-related information about staff in a public facing role. We may also disclose information about staff members whose work is purely administrative if their names are routinely sent out externally.

It is less likely that information about those who do not deal directly with the public in an operational capacity will be disclosed.

The Executive Team and the Senior Leadership Team will have more information disclosed about them, such as photographs and biographical detail, due to their position at NSCHT.

We will consider withholding information if we think that it will prejudice our role or the rights and safety of our staff, irrespective of grade or position.

The type of information you can expect we will disclose is as follows:

- Name and work contact detail
- Pay bands (not your exact salary)
- How long you have worked at NSCHT, your current role, any previous roles or secondments and what your role involves
- Your position in the corporate structure
- Business related entries in your diary/calendar
- Summaries of expense claims without details of where you stayed, where you ate or your itinerary
- Any work-related training at NSCHT
- Any work-related opinions, for example case notes containing your opinion about an investigation or a complainant

The list above does not include every area where we might disclose information about you. The type of information provided will only concern your professional life at NSCHT. We will not disclose non-work related personal or special category data.

When we are asked to disclose diary or calendar information consideration will be given to the safety of our staff. Where this information is requested outside of an FOI request our staff are advised to consult with their manager before sharing information about a staff member, especially when it concerns movements or whereabouts.

We will consult with you prior to deciding whether to disclose any information that we consider would not be within your reasonable expectations.

Before you begin working for us, contact the People Operations Team if you need to make us aware of a specific reason why your information cannot be provided as part of a disclosure. At any later point, if you have any concerns about information being released you need to inform us of this fact.

Requests for references

If you leave, or are thinking of leaving, we may be asked by your new or prospective employers to provide a reference. For example, we may be asked to confirm the dates of your employment or your job role. New employers are obliged to seek consent from the applicant BEFORE requesting a reference from the existing employer. We would not discuss this with an individual prior to releasing the reference.

In relation to employment references, where an employment reference is given in confidence, current data protection legislation creates an exemption from:

- The right to be informed (privacy information)
- The right to make a subject access request

This means that in the UK, if an employment reference is given in confidence and the employee makes a subject access request, both the organisation who issues the reference and NSCHT in receiving it would be exempt from having to provide a copy. NSCHT is not obliged to divulge a reference given to a new employer under a SAR.

Agency Managed Job Applications

If a vacancy is managed by an agency, we will share your data with Optima Health, Civica (TRAC) and Capita (DBS checks) for employment purposes, with your permission.

What are your data protection rights?

Under data protection law, you have rights including:

Your right to be informed – as a controller, we are required to inform individuals when their personal data is collected and about the intended purposes behind the processing of that data. This privacy notice ensures that as an organisation, we satisfy this right.

Your right of access – you have the right to request access to and/or copies of your personal data we hold about you, free of charge (subject to exemptions) – this is known as a subject access request.

How to access your personal data

To request a copy or request access to the personal data we hold about you please use one of the following contact methods:

Register and log into our subject access request portal via our website: www.combined.nhs.uk

Post: Information Governance Department, North Staffordshire Combined Healthcare NHS Trust, Lawton House, Bellringer Close, Trentham, Stoke-on-Trent ST4 8HH

Tel: 0300 123 1535

Email: IG@combined.nhs.uk

Verbal Request: You can make a verbal request for your data but you will not be able to take away your physical file. Your request will be handled in conjunction with your line manager at the site at which you are based. We will consult internally with members of staff who might hold personal data about you.

Your right to rectification – you have the right to have inaccurate (incorrect or misleading) personal data corrected by us without undue or excessive delay. Taking account of the purposes of the processing, you have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

If however, such requests are linked to legally significant matters, such as confirming legal identity, we may require proof of any alleged inaccuracy before we are able to rectify the data held.

Every time you attend a site operated by us, please check that the correct contact details are recorded for you and be prepared to have data checked at every appointment/telephone call.

Your right to restrict processing – you have the right to ask us to restrict the processing of your personal data when one of the following applies:

- You contest the accuracy of your personal data and we are investigating
- We no longer need your personal data, but you need it to be kept for legal claims
- The processing is unlawful, but you oppose erasure of your personal data
- You have objected to us processing your personal data and we are considering whether our legitimate grounds override yours

Your right to object to processing – You have the right to object to us processing your personal data on grounds relating to your particular situation and to data processed for direct marketing purposes where the processing is based on:

- legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

This right does not apply where we can demonstrate compelling legitimate grounds for the processing of your personal data.

If we did not process any personal data about you and your health care needs, it would be very difficult for us to care for and treat you.

Our lawful reasons for using your information mean that the rights that deal with automated decision making, data portability and erasure do not apply.

Transfers of your personal data

We don't routinely transfer staff data overseas but in the rare instances it was deemed necessary, we would always ensure that we have appropriate safeguards in place. In the event that employment is transferred to another employer via TUPE (Transfer of Undertakings, Protection of Employment) Regulations 2006, your personal file and electronic data held on ESR will be transferred to the new employer. We will seek your consent before such a transfer takes place as part of the statutory consultation process.

Third-party processors

We will use carefully selected third-party service providers, as necessary. When we use a third-party service provider to process data on our behalf, we will always have an appropriate agreement in place to ensure that they keep the data secure, do not use or share it other than in accordance with our instructions and that they are operating appropriately.

These third-party service providers include companies that provide IT services and support (including our core clinical systems), systems that manage patient facing services, data hosting service providers, systems that facilitate appointment bookings or electronic prescription services, document management services, delivery services, payment providers and confidential waste companies. This list is not exhaustive and further details of our third-party processors can be supplied on request.

Complaints and your right to complain to the regulator

You can complain directly to us if you are concerned about how we process your personal data. In the first instance, a complaint should be made to our Data Protection Officer.

You can also raise a complaint with the Patient Experience Team, who are available Monday-Friday 9am-5pm.

You also have the right to lodge a complaint with the UK's independent authority on data protection issues, the Information Commissioner's Office.

Data Protection Officer

North Staffordshire Combined Healthcare NHS Trust

Lawton House

Bellringer Road

Trentham

Stoke-on-Trent ST4 8HH

Email: DPO@combined.nhs.uk

Patient Experience Team

Email: patientexperienceteam@combined.nhs.uk

Telephone: 01782 275301

Freephone: 0800 389 9676

Text: 07718 971 123 (please note that this text service is available Monday to Friday 9am-5pm only and is charged at your provider's rate)

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Telephone: 01625 545745 www.ico.gov.uk