



North Staffordshire Combined Healthcare NHS Trust Staff Privacy Notice

As an employer North Staffordshire Combined Healthcare NHS Trust (NSCHT) must meet its contractual, statutory and administrative obligations. We are committed to ensuring that the personal data of our employees is handled in accordance with key Information Governance policies and the principles set out in the Information Commissioner's Office (ICO) [Guide to Data Protection](#)

This privacy notice tells you what to expect when NSCHT collects personal information about you. It applies to all employees, ex-employees, agency staff, and contractors, staff members on secondment and non-executive directors. However the information we will process about you will vary depending on your specific role and personal circumstances.

NSCHT is the data controller for this information unless this notice specifically states otherwise.

This notice should be read in conjunction with the Trust Privacy Notice and other corporate policies and procedures.

How do we get your information

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.

What personal data we process and why

Information related to your employment

We use the following information to carry out the contract we have with you, provide you access to business services required for your role and manage our human resources 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.
- Your date of birth, gender and NI number.
- A copy of your passport or similar photographic identification and / or proof of address documents.
- 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 NSCHT site will be your base)
- 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.

Information 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 maternity leave.

- Information 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.



Information relating to your performance and training

We use this information 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.

- Information 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.
- Information related to your training history and development needs.

Information relating to monitoring

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

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

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

We use the following information 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.
- Accident records if you have an accident at work.
- Details of any desk audits, access needs or reasonable adjustments.
- Information you have provided regarding Protected Characteristics as defined by the Equality Act 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.



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 the GDPR:

- 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.

Criminal convictions and offences

We process information about staff criminal convictions and offences. The lawful basis we rely 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.



How long we keep your personal data

For information about how long we hold your personal data, see our Records Management Policy, which adheres to the [Records Management Code of Practice 2021](#)

Data Sharing

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.

Do we use any data processors?

Yes - a list of our current main data processors can be found in Appendix A.

Your rights in relation to this processing

As an individual you have certain rights regarding our processing of your personal data, including a right to lodge a complaint with the Information Commissioner's Office as the relevant supervisory authority.

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

Right to access your personal information– you can request access to and/or copies of the personal data we hold about you, free of charge (subject to exemptions). We will aim to provide your information within one calendar month as required by the Data Protection Act 2018 and will notify you if this is not possible for whatever reason. Requests can be made verbally or in writing, but we do ask that you provide us with adequate information to process your request, such as providing full name, address, date of birth, NHS number and details of your request and, where necessary, any documents to verify your identity.

Right to rectification - The correction of personal data when incorrect, out of date or incomplete will be rectified by the Trust without undue or excessive delay. 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 information held.

Right to erasure - Under Article 17 of the UK GDPR individuals have the right to have personal data erased or deleted. This is also known as the 'right to be forgotten'. The right is



not absolute and only applies in certain circumstances, for example when your personal data is no longer necessary for the purpose which it was originally collected or processed for, or if you wish to withdraw your consent after you have previously given your consent.

Right to restrict processing – Article 18 of the UK GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that you can limit the way that the organisation uses your data. This is an alternative to requesting the erasure of your data.

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction.

Right to data portability – Under UK GDPR, individuals have the right to data portability in situations where the personal data that they have provided to the Trust is processed by automated means on the basis of consent, or where the personal information is necessary for the performance of a contract. Individuals are entitled to have their personal information transmitted directly from one data controller to another if it is technically feasible to do so. This means being in a structured, commonly used and machine-readable format.

Right to object to processing – individuals have the right to object to the processing of their personal information on grounds relating to their particular situation and to data processed for direct marketing purposes, however if we can demonstrate compelling legitimate grounds to process the information then processing can continue. If we did not process any personal information about you and your health care needs it would be very difficult for us to care for and treat you.

Rights in relation to automated decision making and profiling - Automated individual decision-making is a decision made by automated means (i.e., a computer system) without any human intervention. If any of the processes we use rely on automated decision making, you do have the right to ask for a human to review any computer-generated decision at any point.

Transfers of personal data

We don't routinely transfer staff personal data overseas but in the rare instance it was deemed necessary we would always ensure that we have appropriate safeguards in place.

Personnel files

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

Subject Access Request for Personal Employment Information

You can request your personnel file by emailing the Information Governance team or by submitting a subject access request to NSCHT.informationgovernance@combined.nhs.uk

You can also make a verbal request for your information. 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.



Car park scheme

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 exactly the same way as any staff information, ensuring adherence to strict confidentiality requirements at all times.

Staff surveys

The data collected from staff surveys is processed by Quality Health. Any data collected by Quality Health for us is stored on UK servers. A link to their privacy notice can be found in Appendix A

Most survey questions require quantitative responses, however some free text boxes are included. We would advise you not to share identifiable information about yourself in these boxes if you wish to remain anonymous.

Whistleblowers

NSCHT has a policy and procedure in place to enable its current staff and ex-employees to have an avenue for raising concerns 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.

Equal opportunities monitoring

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 NSCHT. A link to their privacy notice can be found in Appendix A.

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.

Workforce Development and Planning

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. Links to their privacy notices can be found in Annex A. We will share some information about you with these providers both prior to you joining NSCHT 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.

Occupational Health

During your employment you may be referred to occupational health following a request to HR by you or your line manager. This may result in a face-to-face consultation, a telephone appointment with an occupational healthcare professional and/or a medical report from a GP or specialist.

We use TP Health to provide our occupational health service. The information you provide will be held by TP health, who will give us a fit to work certificate or a report with recommendations. A link to their privacy notice can be found in Appendix A.

Trade Union Membership

The recognised unions at NSCHT (Unison) are controllers for the personal information connected to your union membership. NSCHT holds some union subscription details in order to process salary deductions for union membership for which you will have given your consent.

Monitoring of staff

All of our ICT systems and the door access system for the entry and exit of our premises are auditable and can be monitored.

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.

Security clearance

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).

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.

Identification/Access Passes

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 NSCHT 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 NSCHT your details are deleted as soon as possible from this system as part of the leaver's process.

CCTV

We operate CCTV outside of our Lawton House premises to monitor access to certain areas outside of the offices. Further information is available in our CCTV policy. 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. NSCHT is not the data controller for this information.

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 details.
- 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 due 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 at the NSCHT, contact HR 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. If you are still employed by us at the time the request for a reference is received we will discuss this with you before providing this.

In relation to employment references, where an employment reference is given in confidence, the Data Protection Act 2018 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.

Concerns/Complaints

Should you have any concerns about how your personal employment information is managed, please contact the Trust's Data Protection Officer in the first instance:

Data Protection Officer: Mrs. Elizabeth Griffiths, North Staffordshire Combined Healthcare NHS Trust, Lawton House, Bellringer Road, Trentham, Stoke-on-Trent ST4 8HH

Tel: 0300 123 1535 **Direct DPO e-mail:** liz.griffiths@combined.nhs.uk



You also have the right to lodge a complaint with the UK's independent authority on data protection issues, the **Information Commissioner's Office** using the contact details below, and quoting the NSCHT ICO registration number of **Z8606519**:

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

Tel: 01625 545745

Website contact: <https://ico.org.uk/>



Annex A – Data Processors

Data processors are third parties who we instruct to provide staff services for us. We have contracts in place with them and they cannot do anything with your personal information unless we have instructed them to do so. Our main current data processors are listed below:

Data Processor	Purpose	Privacy Notice
Midlands and Lancashire Commissioning Support Unit (MLCSU)	Provider of payroll services	https://www.midlandslancashirecsu.nhs.uk/privacy
Staffordshire and Shropshire Health Informatics Service (SSHIS)	Provider of our managed IT service for our IT infrastructure	https://www.sshis.nhs.uk/our-privacy-policy
NHSBSA	For administering NHS Pensions	https://www.nhsbsa.nhs.uk/our-policies/privacy
TP Health	Occupational Health Provider	https://tphealth.co.uk/privacy-statement/
Government Childcare Voucher Services	Childcare voucher provider	https://www.gov.uk/help/privacy-notice
Her Majesty's Revenue and Customs (HMRC)	Security clearance applications	https://www.gov.uk/government/publications/data-protection-act-dpa-information-hm-revenue-and-customs-hold-about-you/data-protection-act-dpa-information-hm-revenue-and-customs-hold-about-you
Traineasy – Learning Management System (LMS)	Training provider	http://traineasylms.com/privacy-policy/
Quality Health	Staff Surveys	https://quality-health.co.uk/data-protection/