



Privacy Notice Employee and Volunteer Information

Introduction

North West Boroughs Healthcare NHS Foundation Trust aims to be as transparent as possible and provide people with accessible information about the Trust, why it needs to collect data, what it does with the data, who it will be shared with and how and for how long it will be held. This notice is for all employees, contractors, appointees and volunteers.

This privacy notice is intended to answer most common questions, but if further information is required please contact the Trust's Information Governance Team by emailing DPO@nwbh.nhs.uk or telephoning 01925 664485.

Who Are We?

North West Boroughs Healthcare NHS Foundation Trust is a public organisation that provides treatment, support and guidance for a range of health needs for people, both children and adults, living in Greater Manchester, Halton, Knowsley, Sefton, St Helens, Warrington and Wigan. The health needs include physical and mental health conditions and learning disabilities.

The Trust has a statutory responsibility and public duty to provide health care services, as instructed and guided by the Department of Health and Social Care (a ministerial department of Government within the United Kingdom).

The Trust's main address is:

Hollins Park
Hollins Lane
Winwick
Warrington
WA2 8WA

The Trust can be contacted at:

Main Switchboard:	01925 664000
Trust Website:	www.nwbh.nhs.uk

The Trust is a Data Controller and, as such, is registered with the Information Commissioner's Office (ICO). Its registration number is Z8591053.

The Trust's Data Protection Officer (DPO) is the Information Governance & Security Manager, who is supported in this role by the Information Governance Team. The DPO can be contacted by emailing DPO@nwbh.nhs.uk or phoning 01925 664485.

Why does the Trust need your Information?

During the course of its employment activities, the Trust collects, stores and processes personal information about prospective (applicants), current and former staff (including agency, casual and contracted staff), volunteers, trainees and those carrying out work experience. This information enables the organisation to be run effectively.

The Trust recognises the need to treat staff personal and confidential information in a fair and lawful manner and no information will be processed unless these requirements can be met.

What will it be used for?

The Trust will process your data in order to:

- recruit staff, volunteers and contractors and check legal entitlement to work in the UK,
- retain, develop, educate and train staff and volunteers (eg evaluate performance, decide on promotions, manage development and training and retain staff),
- pay staff (including the provision of any additional agreed benefits or salary sacrifice schemes), deduct tax and national insurance contributions and administer pensions,
- undertake equality, diversity and inclusion monitoring,
- process union fee salary deductions and liaise with trade unions (where staff are members of a union and have union fees deducted from their salary),
- manage sickness absence, assess fitness to work, provide relevant occupational health services and undertake adaptations where necessary,
- undertake service evaluation (including analysing data for workforce planning, staff retention and development of staff),
- manage the Trust's business, accounting and audit,
- process expenses claims or to book work-related travel and/or accommodation,
- carry out background checks to ensure the suitability of employees to work in the Trust (where appropriate using information from statutory bodies such as the Disclosure and Barring Service for England and Wales),
- ensure security and safety (eg for the prevention and detection of fraud and other serious crimes, assisting in the prevention and control of diseases, or recording images on CCTV cameras),
- conduct grievance or disciplinary processes, manage complaints and concerns and handle legal claims and incidents,
- provide and monitor network and ICT systems, and
- manage the termination of the working relationship between the individual and the Trust.

Please note that the Trust does not use automated decision-making services (where decisions are made based on your personal data without any human intervention).

What Data is Held?

There are two types of data that the Trust uses: personal and special category. Personal data means any information relating to a person who can be directly (eg by name or picture) or indirectly (eg by age, gender and post code) recognised. Special category data means any information relating to racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life or details of criminal offences.

In order to carry out its activities and obligations as an employer and a business, the Trust handles data in relation to:

- personal demographics (including date of birth, gender, race, ethnicity, sexual orientation, religion, marital status and family details),
- contact details (such as names, addresses, telephone numbers, email addresses and emergency contact details),
- employment records (including recruitment information, employment history, professional membership, references and proof of eligibility to work in the UK and security checks),
- workplace location and contact details, including telephone numbers and email addresses,
- identity badges and smart and swipe card records,
- National Insurance Number,
- bank details,
- payroll and pension details (including tax information),
- photographs and CCTV images,
- absence and sickness information,
- benefits information (including salary sacrifice schemes, vouchers, etc),
- driving licence details and vehicle information (including insurance, road tax and MOT details),
- training records and performance evaluations,
- medical information (occupational health information including physical or mental health conditions, sickness records and information required for reasonable adaptations),
- network user account information and network, communications and Internet usage history,
- information relating to health and safety,
- trade union membership,
- offences (including alleged offences), criminal proceedings, outcomes and sentences, and
- employment tribunal applications, disciplinary and grievance records, records of compensation payments, complaints, accidents, and incident details.

Your information will primarily be held electronically. When registering for NHS employment, all staff are registered on a national database - the Electronic Staff Record (ESR), which is an integrated Human Resources and Payroll System for the NHS provided by NHS Business Services Authority. The Trust also uses other databases (eg TRAC, SimpleSAF and Therefore) that it is responsible for, either directly or through legal contracts with suppliers, to hold and process information about its employees.

Information within these databases is held securely and confidentially, with access restricted to only relevant staff and managers. Confidential information can be accessed via these databases and information is routinely transferred between these databases that includes copies of confidential documents (eg bank statements, birth certificates, driver's licence, etc).

Some records are still held in paper format, particularly historical personnel records. These are stored securely and may be transferred to electronic format at some point.

Lawful Basis for Processing

Under current Data Protection legislation (the Data Protection Act 2018 [DPA 2018] and the General Data Protection Regulation [GDPR]) the Trust will process the following types of information for the legal bases specified.

Type of Information	Legal Basis for Processing (within GDPR)
Staff administration and management (including recruitment, Disclosure and Barring Service checks and performance)	<p>Personal data processing is necessary for: Article 6(1)(b) – “Contractual necessity”</p> <p>Special category data processing is necessary for: Article 9(2)(b) – “Employment and social security” purposes</p>
Payroll and pensions administration ¹	
Education and training	
Trade unions	<p>Personal data processing is necessary for: Article 6(1)(a) – “Consent”</p> <p>Special category data processing is necessary for: Article 9(2)(a) – “Explicit consent”</p>
Occupational health	Refer to the <i>Privacy Notice – Occupational Health Services</i> .
Public health (The Trust has an obligation to protect the health of the general public.)	<p>Personal data processing is necessary for: Article 6(1)(e) – “Public interest”</p> <p>Special category data processing is necessary for: Article 9(2)(i) – “Public health” purposes</p>

¹ The Trust's Payroll Service is outsourced to St Helens & Knowsley Teaching Hospitals NHS Trust.

Type of Information	Legal Basis for Processing (within GDPR)
Crime prevention and prosecution of offenders	<p>Personal data processing is necessary for: Article 6(1)(e) – “Public interest”</p> <p>Special category data processing is necessary for: Article 9(2)(g) – “Substantial public interest” purposes</p> <p>The following legal bases apply when necessary and proportionate to safeguard someone else: Article 23(1)(d) – “the prevention, investigation, detection or prosecution of criminal offences...” Article 23(1)(e) – “other important objectives of public interest (including monetary, budgetary and taxation matters, public health and social security.”</p>
Sharing and matching of personal information for national fraud initiative	

There may be occasions where the Trust needs to process personal and/or special category data because someone is at risk of serious harm (eg life or death situations in emergencies or major incidents) and, where we do this, we will process the information to “protect someone’s vital interests” (Articles 6(1)(d) and 9(2)(c)).

There may be occasions when we will be obliged to process your information in order to comply with a court order, coroner’s instruction, to prevent or detect crime or to comply with the law (eg to provide the Secretary of State with information and reports on the status, activity and performance of the Trust). Where we do this we will process your personal and/or special category data to comply with a legal obligation to which the Trust is subject (Article 6(1)(c)).

If we process your information for other purposes that are not described above then we will seek your consent to do so before we process it (for example, sharing information with Trade Unions).

If the Trust wishes to use your personal information for a new purpose that is not covered by this Privacy Notice, then we will provide you with a new notice explaining the new use prior to commencing the processing, setting out the relevant purposes and processing conditions. Where and whenever necessary, we will ensure there is a legal justification for such processing.

Who do we Share Data with?

The types of organisations and people the Trust may share your data with include (but are not limited to):

- payroll and pension provider(s),
- companies who provide contact centres and help desks,
- IT service providers,
- couriers and delivery companies,
- professional advisors, including accountants, solicitors and management consultants,
- other healthcare professionals (eg in relation to occupational health, etc),

- other NHS organisations if you accept employment with them (see “Streamlining” Section below),
- NHS managers and the Department of Health/NHS Digital for the purposes of planning, commissioning, managing and auditing healthcare services,
- organisations we contract with to provide services to or on behalf of the Trust,
- other organisations where TUPE rules apply (see below),
- bodies with statutory investigative powers (eg NHS Resolution, the Care Quality Commission, General Medical Council, Nursing and Midwifery Council, Audit Commission or Health Service Ombudsman),
- Government departments for national screening programmes and other national initiatives (eg NHS England, Public Health England or the Home Office), and
- police, emergency and out-of-hours services, courts (including coroner's court), solicitors and tribunals and enquiries.
- Disclosure and Barring Service
- Government departments (eg HM Revenue and Customs, Department for Work and Pensions, UK Visas and Immigration, etc)
- Care Identity Service
- Trade Unions

Any disclosures will be considered on a case-by-case basis to determine if they are appropriate and what the legal basis is for sharing. If the sharing goes ahead, only the minimum personal data necessary for the specific purposes and circumstances will be shared, with all suitable security controls in place. Any organisations receiving person-identifiable information from us are legally obligated to protect it.

The Trust will not share your information for marketing, social media or insurance purposes unless it has your consent to do so. If you do consent to this, you have the right to withdraw your consent to the processing at any time.

Staff names, job titles, work contact details and pay bands are not confidential and are subject to release under the Freedom of Information Act 2000 upon request.

Looking after your Information

The Trust takes its duty to protect your personal information and confidentiality very seriously and we are committed to taking all reasonable measures to ensure it is kept confidential and secure and used appropriately. Everyone working for the NHS has a contractual and legal duty to protect your information.

Personal information is held in accordance with the requirements of current Data Protection legislation. Anyone who receives information from us is also under a legal duty to keep it confidential and secure in accordance with Data Protection legislation.

We strive to ensure that all personal information under our control is handled in accordance with all legal, professional and ethical obligations. Policies and procedures are in place to safeguard information, which staff are responsible for

adhering to, and all staff are provided with mandatory training to assist them in fulfilling their obligations.

Access to personal information is strictly controlled and restricted to only those with a legitimate work related need to access it.

Streamlining and Inter Authority Transfers

Streamlining is about delivering a quality recruitment experience in an efficient and timely way, reducing duplication and unnecessary delays in getting the successful candidate started in the workplace. Streamlining includes data sharing arrangements aimed at saving time for individuals when their employer changes, as well as improving efficiencies and making cost savings for the NHS as a whole. To facilitate this, the Trust has implemented effective streamlined human resources processes for all NHS-to-NHS staff transfers and to manage doctors in training rotations.

The Electronic Staff Record Inter Authority Transfer (IAT) is an automated process that allows employee information to be shared between NHS organisations when an individual accepts an offer of employment elsewhere or their employment transfers.

In accepting employment with the Trust, you agree to the following personal data being transferred under the streamlining programme and IAT process if your employment (permanent or temporary) transfers to another NHS organisation. You have the right to object to your information being shared (see below).

Type	Reason for Transfer
Personal information (eg name, address, National Insurance number, etc)	To enable the new NHS employer to verify who you are.
Employment information (eg pay grade/banding, employment dates, salary, post, sickness information, etc)	To enable the new NHS employer to ensure you are paid correctly and can calculate appropriate NHS holiday and sickness entitlements.
Training compliance and competency information	So staff should not need to repeat some nationally recognised training, including statutory and mandatory/core skills training.

Please be advised that immunisation and vaccination data is not currently transferred in all organisations, but may be in future. You will be notified of this change before it is implemented.

TUPE (Transfer of Undertakings)

The TUPE rules apply to organisations of all sizes and protect employees' rights when the organisation or service they work for transfers to a new employer. When TUPE applies, the employees of the organisation making the transfer automatically become employees of the incoming employer at the point of transfer. They carry

with them their continuous service from the outgoing employer, and should continue to enjoy the same terms and conditions of employment with the incoming employer.

Should the Trust have to transfer any staff to another organisation, it must provide information about transferring employees to the incoming employer, no less than 28 days before the transfer. This is called Employee Liability Information and includes:

- the identity and age of the employees who will transfer,
- information contained in the written statement of those employees,
- details of any disciplinary action taken against an employee in the last two years,
- details of grievances raised by an employee in the last two years,
- instances of legal actions taken by employees against the outgoing employer in the last two years (any court or employment tribunal claims),
- Occupational Health information, and
- information regarding any collective agreements.

Foundation Trust Membership

Staff are automatically enrolled as members upon joining the Trust. However, they can opt-out upon request to the Foundation Trust Membership Office (this does not apply to non-executive directors who must be public members). Please see the *Privacy Notice – Foundation Trust Membership* for further information.

Safeguarding

Some members of society are recognised as needing protection, for example children and vulnerable adults. If a person is identified as being at risk from harm The Trust must do what it can to protect them.

Where there is a suspected or actual safeguarding issue the Trust will share relevant information that it holds with other relevant agencies, regardless of whether or not the individual or their representative agrees. The laws that allow this processing to be undertaken without consent are the Children Act 1989 (Section 47) and the Care Act 2014 (Section 45).

Your Rights

Right to Access

You have the right to access the data held about you, except for information that:

- has been provided in confidence by someone else without consenting for you to see it,
- relates to serious criminal offences, and/or
- could cause physical or mental harm to you or someone else.

To request access to records the Trust holds, please contact the Information Governance Team by emailing AccessToRecords@nwbh.nhs.uk or phoning 01925 664844.

Right to Data Portability

This only applies to information you have given us. You have the right to ask that we transfer the information you gave us from one organisation to another, or give it to you. The right only applies if we are processing information based on your consent or under, or in talks about entering into a contract and the processing is automated (Article 6(1)(a) and (b)).

Right to Erasure

You have the right to ask us to erase your personal information in certain circumstances (when processing is being undertaken in compliance with Article 6(1)(a), (b) or (d)).

Right to Object

People who have access to your information will only normally have access to that which they need to fulfil their roles. You have the right to object to processing if the processing forms part of our public tasks, or is in our legitimate interests (Article 6(1)(e)). However, the Trust may still share information even if you have objected where there is a valid legal justification (eg someone is at serious risk).

If you wish to object to the sharing of your information as part of streamlining and the IAT process, please contact the Trust's Resourcing Team.

Right to Rectification

You have the right to ask us to rectify information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete. For further information please speak to your line manager in the first instance. Further guidance can be obtained from the Information Governance Team by emailing Records@nwbh.nhs.uk or phoning 01925 664895.

Further Information on your Rights

For further information regarding your rights, please see the ICO's website: <https://ico.org.uk/global/privacy-notice/your-data-protection-rights/>. Alternatively, you can contact the Trust's Information Governance Team by emailing IG@nwbh.nhs.uk or phoning 01925 664485.

Retention Period

The Trust retains the information it holds in line with the Records Management Code of Practice for Health and Social Care 2016², following which it usually be confidentially destroyed.

Transferring Information Abroad

The Trust does not routinely transfer information outside the UK, but if there is a need to do so it will be done in a way that ensures the security of the information is to an equivalent standard as that used internally by the Trust when processing your information.

Trust Website

You can browse the Trust's website without disclosing personal data. However, the Trust may store information about you using cookies, which are small text files that are placed on your computer by websites that you visit. They are widely used in order to make websites work, or work more efficiently, as well as to provide information to the owners of the site. To find out more about cookies, including how to see what cookies have been set, visit www.aboutcookies.org or www.allaboutcookies.org.

The Trust also uses Google Analytics³ to collect information about how visitors use its website. The information is used to compile reports and to help improve the website. The cookies collect information in an anonymous form, including the number of visitors to the website, where visitors have come to the website from and the pages they visited. To opt out of being tracked by Google Analytics across all websites, visit <http://tools.google.com/dlpage/gaoptout>.

The Trust's website contains links to other (external) sites. The Trust is not responsible for the privacy practices and content of these sites. The Trust encourages you to be aware of this when you leave its site and to read the privacy statements on the other websites.

Closed Circuit TV (CCTV)

The Trust uses Closed Circuit TV to help reduce the fear of crime for patients, staff and visitors to its sites and to protect its premises and assets from criminal activity. In addition, CCTV may be used to monitor difficult to observe areas where patient or public safety could be compromised. If an incident occurs, the CCTV footage may be shared with the police for the purposes of investigating a crime. However, the Trust ensures that the use of CCTV complies with all relevant regulatory acts of law.

² <https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016>

³ <https://policies.google.com/privacy/update>

Right to Complain

The Trust aims to make sure that the services it delivers are provided to the highest standard. If you have any concerns about the way the Trust has handled its data, you can raise your concerns or make a complaint.

- To raise a complaint, please speak to your line manager or your Freedom to Speak Up Champion or Guardian, in the first instance.
- To raise a concern, please contact the Information Governance Team by emailing IG@nwbh.nhs.uk or phoning 01925 664485.
- To make an external complaint about the Trust's data handling, please contact the ICO by emailing casework@ico.org.uk or phoning 0303 123 1113.