

Staff Privacy Notice

At Northampton General Hospital NHS Trust, we are committed to ensuring that we collect, store and process personal information about prospective, current and former staff in line with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

Information we collect about you

The Trust collects, holds and processes personal data and sensitive data about its current, past or prospective staff including substantive staff, bank and agency workers, contracted staff, volunteers, trainees and those carrying out work experience from recruitment to employment and beyond.

Types of personal data we hold

- **Personal data**
The Trust will hold personal data about you for example: Name, address, telephone number, staff number, gender, NI Number, next of kin/emergency contact details, professional membership information, reference information and bank details.
- **Sensitive personal data (special categories)**
The Trust will also hold sensitive personal data including race or ethnic origin, religious beliefs, trade union membership, health, sexual orientation, criminal convictions and disabilities.

Information provided by you

When you apply for a position within the Trust you will provide us with relevant information about you, including:

- Name
- Address and telephone contact details
- Employment history
- Qualifications
- Referee details

During the recruitment and selection process we will begin to add further information including:

- Copies of qualifications/ certificates
- Pre-employment checks, including references, identity documents and 'right to work' information
- Publically available information such as social media presence
- Selection information including correspondence, interview notes, and results of any selection tests etc

- At appointment we secure photographs for smartcards and ID Cards. This photograph may also be used in local/departmental areas and on the hospital intranet page to support with identification for other staff members.

Following your appointment we may add any other information you supply to us or is required as part of your employment such as revalidation information.

Information provided by other sources

Information may be provided about you from a number of sources during your recruitment and on-going employment with the Trust including:

- Disclosure and Barring Service disclosures, where applicable, which will tell the organisation about any criminal convictions you may have
- Referees providing confidential information about your suitability to the role
- Inter Authority Transfer (IAT) – Information held by your previous NHS employer
- Information from HM Revenue and Customs (HMRC) relating to your pay and employment
- Information about your right to work and visa applications
- Pension Information when transferring within the NHS
- Information from your manager and HR team relating to your performance, sickness absence and other work related matters
- Confirmation of your registration with a professional body

Legal basis for processing

The Trust will only ever process your personal information where it is able to do so by law and using one of a number of legal bases available under the Data Protection Act 2018 and General Data Protection Regulation 2016 (GDPR).

The legal basis for processing we use most often are:

1. Legal Obligations – In many cases we have a legal obligation to hold and process information about you for example informing HMRC of the tax and National Insurance Contributions you have made and ensuring the safety and care of our patients and staff. (GDPR Article 6,1(c))
2. Legitimate Interests – In some cases, for example sharing data between NHS organisations. (GDPR Article 6, 1 (f))

Where we process sensitive personal or special categories of data about you (i.e. race or ethnic origin, religious beliefs, trade union membership, health, sexual orientation, criminal convictions and disabilities) we will ensure this is done so using one of the following:

1. Employment Rights – Carrying out obligation's and specific rights required by us as an organisation for the purposes of employment (e.g. monitoring the equality and diversity of our workforce or DBS checking) (GDPR Article 9, 2(b))

2. Preventative or Occupational Medicine – assessing the working capacity of our employees (GDPR Article 9, 2(h))

Your individual rights

You have certain rights with respect to the data held about you by the Trust. These are:

1. To be informed why, where and how we use your information
2. To request access to your information
3. To request for your information to be corrected if it is inaccurate or incomplete
4. To request for your information to be deleted or removed where there is no longer necessary for us to hold it
5. To request that we restrict the use of your information
6. To request that we copy or transfer your information from one IT system to another in a safe and secure way, without impacting the quality of the information
7. To object to how your information is used
8. To challenge any decisions made without human intervention (automated decision making)

In accepting employment with the organisation, you accept that the following personal data will be transferred in accordance with streamlining staff movement principles, if you accept an offer with another NHS organisation, or your employment transfers or is seconded to another NHS organisation the following information will be shared:

- Personal data e.g. name, DOB, address, NI Number, to enable the new NHS employer to verify who you are
- Employment Information e.g. your position, salary, grade, employment dates, dates of any sickness (excluding absence reasons), to enable you to be paid correctly and the new employer to calculate appropriate NHS entitlements for annual leave and sickness
- Training compliance / competency dates, to reduce the need to repeat nationally recognised training and statutory and mandatory training

This information will be shared via the Inter Authority Transfer (IAT) which is the secure process where information is transferred from one NHS employer to another.

How information is accessed and secured

The Trust will use your information to administrate your employment and associated functions, personal data will be shared between relevant colleagues who legitimately need the information to carry out their duties e.g. your line manager and the HR department.

The Trust maintains electronic and paper records relating to your recruitment and employment, with information held by the HR department and locally with your line manager.

All paper files are kept in secure locked cabinets/cupboards and only relevant staff will have access to this information. Electronic information is accessed on a need to know basis only using the Trust's ESR system. Some information may be held on the Trust's secure drives or shared folders where access is only granted to appropriate individuals.

How staff data is used

The Trust uses staff data for all purposes associated with the administration of the employer/employee relationship and to meet our legal obligations. The purposes for which we may use staff data (including sensitive personal information) include:

- Process your recruitment application and correspond with you in relation to Trust vacancies
- Maintaining staff records
- Recruitment and selection
- Managing Human Resource employment matters (e.g. promotion, training and development, conduct, attendance, appraisals, management progress, grievances, misconduct investigations, disciplinary actions and complaints)
- Administering finance (e.g. salary, pension and staff benefits)
- Complying with visa requirements
- Providing facilities such as IT/system access, library services and car parking
- Monitoring equal opportunities
- Preventing and detecting crime, such as using CCTV and using photo's on ID badges
- Providing communication about the Trust, news and events
- Maintaining contact with past employees
- Provision of wellbeing and support services
- Compliance with legal obligations such as making external/statutory returns to NHS England, sharing information with HMRC
- Carrying out research, surveys and statistical analysis (including using third party data processors to carry out the national staff survey)
- To enrol you as a Foundation Trust member
- Carrying out audits

The Trust processes sensitive personal data for a number of administrative purposes:

- Equal opportunities monitoring
- Managing Human Resources/Financial processes such as administering sick pay and sick leave, managing absence, administering Maternity Leave and associated pay schemes
- Managing a safe environment and ensuring fitness to work
- Managing obligations under Equal Opportunities Legislation
- Provision of Occupational Health and Wellbeing service to individuals
- Payment of trade union membership fees

Keeping information up to date

All staff are responsible for ensuring that the information held on ESR is always up to date and should notify their line manager promptly of any changes.

How long is information kept?

The Trust will keep your records for the period of time defined in the Documentation Management Policy (NGH-PO-123).

Sharing information with third parties

The Trust may disclose personal and sensitive information with a variety of recipients including:

- Our employees, agents and contractors where there is a legitimate reason for them receiving the information
- Current, past or potential employers of our staff to provide or obtain references
- Professional and regulatory bodies (e.g. Nursing and Midwifery Council (NMC), Health and Care Professions Council (HCPC), General Medical Council (GMC)) in relation to the confirmation of conduct including complaints, job description and information provided as part of the recruitment process
- Government departments and agencies where we have a statutory obligation to provide information (e.g. HMCR, NHS Digital, Department of Health and the Home Office)
- The Disclosure and Barring Service (DBS) and DBS Update Service where we require a DBS check for certain roles
- Third parties who work with us to provide staff support services (e.g. counselling)
- Crime prevention or detection agencies (e.g. the police, security organisations, department for works and pensions and local authorities)
- Internal and external auditors
- Debt collection and tracing agencies
- Courts and tribunals
- Trade union and staff associations
- Survey organisations for example for the annual national NHS Staff Survey

Any disclosures of personal data are always made on case-by-case basis, using the minimum personal data necessary for the specific purpose and circumstances and with the appropriate security controls in place. Information is only shared with those agencies and bodies who have a "need to know" or where you have consented to the disclosure of your personal data to such persons.

Using your photograph

If you agree to your photograph being taken, or taking part in a video for trust purposes, we will first seek your consent to publish, republish, transmit or broadcast any still and/or video images and audio recordings across a range of print, online, broadcast and social media channels to promote the principles and practices of the hospital. We will also seek your consent to storing images and recordings in the NGH photo library for three years.

Sharing information with the NHS business service authority

The Trust also shares employee records information with NHS Business Services Authority. The information which you provide during the course of your employment (including the recruitment process) will be shared with the NHS Business Services Authority for maintaining your employment records, held on the national NHS Electronic Staff Record (ESR) system.

On commencement of employment with the organisation, your personal data will be uploaded into the ESR system. ESR is a workforce solution for the NHS which is used by the organisation to effectively manage the workforce, leading to improved efficiency.

Further information

If you wish to ask the Trust about a data protection issue, request information on data we process, request a copy of your data, make a request for data to be erased, rectified or you have concerns about the processing of your personal data by us you may contact:

The Data Controller

The Chief Information Officer & SIRO
Northampton General Hospital NHS Trust
Cliftonville
Northampton, NN1 5BD
Telephone: 01604 634 700

Information Governance Team

Northampton General Hospital
Cliftonville
Northampton, NN1 5BD
Telephone: 01604 543881
Email: dataprotectionact@ngh.nhs.uk

Data Protection Officer

Northampton General Hospital
Cliftonville
Northampton, NN1 5BD
Telephone: 01604 523224
Email: dpo@ngh.nhs.uk

If you are still unhappy with the outcome of your enquiry you can write to:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire, SK9 5AF
Telephone: 0303 123 1113

