

## Staff Privacy Notice

University Hospitals of North Midlands NHS Trust ("the Trust") is committed to protecting the personal data of its employees. This Notice sets out important information about how the Trust ("the Trust" or "we" or "us") collect and use your personal data during the course of your employment and after your employment has ended.

This privacy notice is intended for employees of the Trust as well as bank workers, employees who have left the organisation, staff on honorary contracts, staff seconded into and out of the organisation, students, and people undertaking work experience at the Trust.

You should read this Notice carefully and raise any questions you may have with the HR Directorate (e-mail [myemployeerelations@uhn.nhs.uk](mailto:myemployeerelations@uhn.nhs.uk)) or Information Governance (e-mail - [infogovuhnm@uhn.nhs.uk](mailto:infogovuhnm@uhn.nhs.uk))

### Scope of the Privacy Notice

In connection with your employment, the relevant Data Controller is the University Hospitals of North Midlands NHS Trust

Personal data means information which identifies you and relates to you as an individual.

As your employer, the Trust will collect, use and store your personal data for a wide variety of reasons in connection with the employment relationship.

- Your personal details such as your name, address, telephone numbers, personal email address and date of birth, next of kin details in order to administer your employment, manage our business and ensure that we can contact you in an emergency
- Terms and conditions of your employment
- Your national insurance number, tax and bank details, in order to pay you and details of your pension in order to enrol you onto the relevant scheme
- Information about your skills, qualifications, employment history, experience and (where relevant) professional membership, training history in order to verify your skills and to comply with our legal obligations
- Your nationality and immigration status to confirm your eligibility to work in the UK
- Information about your remuneration, including entitlement to benefits
- Trade union membership
- Information about any criminal record
- References
- Medical information relevant to your employment, including physical health, mental health and absence history - in order to monitor sick leave and take decisions about your fitness to work as well as whether or not you have a disability for which the Trust needs to make reasonable adjustments
- Information relating to your health and safety at work, and any incidents or accidents
- Equal opportunities monitoring information, including information about ethnicity, gender, health, religion or sexual orientation, in order to monitor our compliance with equality legislation

- Details of your working patterns (days of work and working hours) and attendance at work to ensure correct pay
- Details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave
- Details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you (including tribunal claims) and related correspondence
- Assessments of your performance, including PDRs/appraisals, performance reviews and ratings, performance improvement plans and related correspondence;
- Photographs and visual images, personal appearance and behaviour, for example if CCTV images are used as part of building security and ID badges

The Trust collects this information in a variety of ways, for example:

- Documents gathered during the recruitment process (including cv, application form, references, professional memberships and qualifications, background vetting information)\*
- Documents maintained and updated during your employment relating to professional memberships and qualifications and statutory and mandatory training (including but not limited to professional revalidation) \*
- General employment records including details of training, disciplinary and grievance matters, benefits, holiday and other absences, along with a copy of your employment contract, performance records (including PDR/appraisal documentation) and compensation history\*
- Information gathered through the Trust's monitoring of its IT systems, building access records and CCTV recording
- Personal records/documents such as your passport, driving license or other identity documents\*
- Forms completed by you at the start or during employment (such as new starter form, ID checks, OH referrals, PDR records) \*
- Correspondence with you; interview or other assessment records; in person (through meetings or over the telephone); survey forms, questionnaires or registration forms
- Timesheets, rostering and other time and attendance records\*
- From third parties (previous employer; via recruitment systems 'Trac' and 'NHS jobs'; pensions agency; information from employment background check providers; the Disclosure and Barring Service; professional bodies; medical and GP records; government bodies like HM Revenue and Customs, the Department for Work and Pensions, or the UK Visas and Immigration).
- Personal data which you otherwise voluntarily provide, for example when using your Trust e-mail account

\*Note: The personal data provided by you as listed above as \* is mandatory in order for us to administer the employment relationship and/or comply with statutory requirements relating to immigration or taxation. Failure to provide mandatory personal data may affect our ability to accomplish the purposes stated in this Notice and potentially affect your ongoing employment.

The list set out above is not exhaustive, and there may be other personal data which the Trust collects, stores and uses in the context of the employment relationship. We will update this Privacy Notice from time to time to reflect any notable changes in the categories of personal data which the Trust processes.

The majority of the personal data which we process will be collected directly from you. In limited circumstances your personal data may be provided by third parties, such as former employers, official bodies (such as regulators or criminal record bureaus) and medical professionals.

On commencement of employment with the Trust, your personal data will be uploaded to the Electronic Staff Record (ESR). ESR is a workforce solution for the NHS which is used by the Trust to manage the workforce leading to improved efficiency and improved patient safety.

The Trust uses your personal data for a variety of purposes in order to perform its obligations under your employment contract, to comply with legal obligations or otherwise in pursuit of its legitimate organisational interests. We have set out below the main purposes for which employee personal data is processed:

- the payment of wages and the administration of benefits under the employment contract
- the day to day management of tasks and responsibilities
- to manage and assess performance, including the conduct of annual PDR's/appraisals
- to consider eligibility for promotion or for alternative roles within the Trust
- to comply with legal requirements, such as reporting to HMRC or professional regulators
- to address disciplinary and grievance issues with individual employees
- to protect the Trust's confidential and proprietary information, and intellectual property
- to monitor the proper use of the Trust's IT systems
- to prevent fraud against the Trust and its clients
- to safeguard the interests of the Trust's patients
- to comply with any statutory or regulatory obligations, including but not limited to information provided to the CQC, NHS England, NHS Improvement and regulators of clinical professionals such as the Nursing and Midwifery Council and General Medical Council
- if an organisational transfer or change of ownership occurs

Again, this list is not exhaustive and the Trust may undertake additional processing of personal data in line with the purposes set out above. The Trust will update this Notice from time to time to reflect any notable changes in the purposes for which it processes your personal data.

Everyone working for the NHS is subject to the Common Law Duty of Confidentiality. This means that any information that you provide to us in confidence will only be used in connection with the purpose for which it was provided, unless we have specific consent from you or there are other special circumstances covered by law

### **What special categories of personal data do we process?**

Certain categories of data are considered "special categories of personal data" and are subject to additional safeguards. The Trust limits the special categories of personal data which it processes as follows:

- Health Information

The Trust may process information about an employee's physical or mental health in order to comply with its obligations in connection with employment, in particular to:

- administer sick pay entitlements
- facilitate the assessment and provision of NHS Injury Allowance

- comply with obligations owed to disabled employees
- comply with patient care, health regulatory and health and safety obligations;
- maintain a sickness absence record
- obtain Occupational Health advice and support from the Trust's external Occupational Health Service Provider
- to promote and improve the health, safety, welfare and wellbeing of employees

We will always treat information about health as confidential and it will only be shared internally where there is a specific and legitimate purpose to do so. We have implemented appropriate physical, technical, and organisational security measures designed to secure your personal data against accidental loss and unauthorised access, use, alteration, or disclosure.

Health information will typically be retained in accordance with the **Records Management: Code of Practice for Health and Social Care 2016**, which can be accessed via the following link:

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

- Disclosure and Barring checks/information (DBS)

Given the nature of our organisation, DBS requirements apply to all employees working in the Trust.

We are required to carry out DBS checks for all clinical roles, other regulated roles and for any roles that involve contact with patients in the course of their normal duties. In all cases, we carry out the checks in line with the applicable law.

For clinical and other regulated roles, DBS checks may be repeated periodically during the course of employment in line with Trust Policy and Procedure for the Disclosure and Barring Service Check

We will always treat DBS information as confidential and it will only be shared internally where there is a specific and legitimate purpose to do so. We have implemented appropriate physical, technical, and organisational security measures designed to secure your personal data against accidental loss and unauthorised access, use, alteration, or disclosure.

- Retention of DBS: Once a recruitment (or other relevant) decision has been made, Disclosure information is retained for a period of up to six months, to allow for the consideration and resolution of any disputes or complaints. If, in very exceptional circumstances, it is considered necessary to keep Disclosure information for longer than six months, the Trust will consult with the Data Subject about this and will give full consideration to the data protection and human rights of the individual before doing so. Throughout this time, the usual conditions regarding the safe storage and strictly controlled access will prevail.
- Disposal of DBS: Once the retention period has elapsed, any Disclosure information is immediately destroyed by secure means. However, the Trust may keep a record of the date of issue of a Disclosure, the name of the subject, the type of Disclosure requested, the position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the recruitment decision taken.

- Equal Opportunities Monitoring

The Trust is committed to providing equal opportunities in employment and career progression for all of its employees and from time to time it will process information relating to ethnic origin, race, nationality, sexual orientation and disability, alongside information relating to gender and age, for the purposes of equal opportunities monitoring and gender pay reporting.

We have implemented appropriate physical, technical, and organisational security measures designed to secure your personal data against accidental loss and unauthorised access, use, alteration, or disclosure. In addition, this monitoring and reporting will always take place in accordance with appropriate safeguards as required under applicable law, including:

- the provision of information relating to ethnic origin, race, nationality, sexual orientation and disability for the purposes of monitoring will be voluntary and processed for this purpose only;
- the monitoring and reporting will be conducted on the basis of using anonymised data so individual employees cannot be identified;

When do we share employee personal data?

The Trust will share employee personal data with other parties only in limited circumstances and where this is necessary for the performance of the employment contract or to comply with a legal obligation, or otherwise in pursuit of its legitimate business interests as follows:

- Payroll providers
- Benefits providers
- Background vetting specialists
- Occupational health and staff support providers
- National fraud initiative
- Internal and external auditors
- The Department of Health
- Any applicable regulatory body
- Police Authority
- HMRC and/or any other applicable government body
- Accountants, lawyers and other professional advisers

In cases not governed by regulation or legislation, the employee personal data is shared under the terms of a written agreement between the Trust and the third party which includes appropriate security measures to protect the personal data in line with this Notice and our obligations. The third parties are permitted to use the personal data only for the purposes which we have identified or as is permitted by law, and not for their own purposes, and they are not permitted to further share the data without our express permission.

As an employer within the National Health Service, the Trust may be required to share employee personal data with other Trusts from time to time for the purposes set out in this Notice. In particular, the Trust shares employee personal data for the purposes of facilitating cross-organisation clinical care; operational effectiveness; medical research, and for pre-employment checking purposes.

Occasionally, the Trust may be required to disclose employee personal data in response to Freedom of Information Requests. All staff should be aware that information regarding AfC staff at Band 7 and above will be released if requested. This applies to corporate / Trust information (i.e., work contact details) not personal information. AfC bands and job descriptions will be released for all Trust roles if requested. **[IG08 Freedom of Information Policy]**

The Trust's policy is to retain personal data only for as long as needed to fulfil the purpose(s) for which it was collected, or otherwise as required under applicable laws and regulations. Under some circumstances we may anonymise your personal data so that it can no longer be associated with you. We reserve the right to retain and use such anonymous data for any legitimate business purpose without further notice to you.

The Trust is required to have records management procedures in place that cover the creation, filing, location, retrieval, appraisal, archive and destruction of records, in

accordance with the **Records Management: Code of Practice for Health and Social Care 2016**, which can be accessed via the following link:

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

The Trust will always seek to process your personal data in accordance with its obligations and your rights.

You will not be subject to decisions based solely on automated data processing without your prior consent.

In certain circumstances, you have the right to seek the erasure or correction of your personal data, to object to particular aspects of how your data is processed, and otherwise to seek the restriction of the processing of your personal data. You also have the right to request the transfer of your personal data to another party in a commonly used format. If you have any questions about these rights, please contact your local Information Governance Officer using the details set out below.

You have a separate right of access to your personal data processed by the Trust.

If you want to see your personal data, you should, in the first instance, speak to your line manager. If your line manager is unable or unwilling to agree to the request, you can make a **Subject Access Request** by writing to the Director of Human Resources and including your:

- Full name, address and contact details
- Employee number and/or national insurance number
- Details of the specific information required and any relevant dates.

The HR Directorate have a Standard Operating Procedure in place to ensure that Subject Access Requests are dealt with according to the requirements of the Data Protection Act and GDPR.

You may be asked for information to confirm your identity and/or to assist the Trust to locate the data you are seeking as part of the Trust's response to your request.

Finally, you have the right to raise any concerns about how your personal data is being processed with the Information Commissioner's Office (ICO):

ICO website: <https://ico.org.uk/concerns/>

Telephone 0303 123 1113 or

Email: [casework@ico.org.uk](mailto:casework@ico.org.uk).

The HR Directorate oversees compliance with this Notice in conjunction with the Trust's Information Governance Department to deal with any questions or concerns. If you would like further information about the matters set out in this Notice, please contact the Trust's Information Governance Department or HR Directorate. Contact details are set out below:

Human Resources Email: [myemployeerelations@uhnms.nhs.uk](mailto:myemployeerelations@uhnms.nhs.uk)

Information Governance Email: [infogovuhnms@uhnms.nhs.uk](mailto:infogovuhnms@uhnms.nhs.uk)