

PRIVACY NOTICE FOR STAFF

At Humber Teaching NHS Foundation Trust we are committed to protecting and respecting your privacy. We collect, store and process information about prospective, current and former staff. This notice is to help you understand how and why we collect personal information about you, what we do with the information and how we store it. It also explains the decisions you can make about your own information.

WHAT INFORMATION WE COLLECT ABOUT YOU

Information which the Trust collects and holds about you may include:

- Basic details about you such as name, address, date of birth, emergency contact etc.
- Pre-employment details e.g. application form, interview notes, offer of employment, references, contract, qualifications
- Employment information e.g. correspondence with you, annual leave, training records, career history, appraisals
- Information relating employee relations e.g. disciplinary proceedings, grievance and complaints, tribunal claims etc.
- Information needed for payroll, benefits, pension and expenses purposes
- Information relating to your health and safety at work and any incidents or accidents
- Visual images, personal appearance and behaviour, for example, if CCTV images are used as part of building security.

We may also hold special category information about you such as:

- Medical information relevant to your employment, including physical health, mental health and absence history
- Personal demographics, including gender, race, ethnic origin, sexual orientation, religious or other beliefs and whether you have a disability or require any additional support or adjustments for your employment
- Trade union membership
- Depending on the position you hold with us, we may also collect information in relation to any current or previous criminal offences. Please refer to our [Recruitment and Selection Policy and Procedures](#)

USING YOUR PERSONAL DATA: THE LEGAL BASIS AND THE PURPOSE

We will use your information for the following purposes:

Administer our business

Personal data will be used for employment or removals; pay, discipline, superannuation, work management or other personnel matters. This includes, but is not limited to the following;

- To enable you to be paid
- To enable the development of a comprehensive picture of the workforce
- To inform and develop safe recruitment and retention policies
- To support effective performance management

- To allow better financial modelling and planning
- To enable ethnicity and equality monitoring
- To prevent injury or illness arising from work activities as far as reasonably practicable.
- To share important communications relevant to your role at the Trust and to measure the response to those communications to allow us to continually improve and develop them.

This processing is necessary to **perform our contract with you** (UK GDPR Article 6(1)(b)). This processing is necessary to **carry out employment obligations and rights** (UK GDPR Article 9 (2)(b)).

Occupational Health

Personal information obtained during occupational health assessments is held in strict confidence by the occupational health team protected by the requirements of the Data Protection Act. The information is also covered by the professional codes of conduct of the General Medical Council and the Nursing and Midwifery Council. As a “patient” of the team, the information is protected in the same way as when an individual consults any health care professional.

This processing is necessary to **perform a public task** (UK GDPR Article 6 (1)(e)). The processing is necessary for the **provision of health or social care** (UK GDPR Article 9 (2)(h)).

National COVID-19 and Flu Vaccination Programmes

Information about COVID-19 and flu vaccines received by NHS staff is collected by NHS England and Improvement along with information from your Electronic Staff Record (ESR). This data will only be used to match the ESR record with your vaccine record and to support the purposes of the vaccination programme. It will not be used for any other purpose. Data about your vaccination will only be made available to the health and care organisation that you work for and your GP practice. It will not be accessible to any other health and care organisations.

This processing is necessary for **compliance with a legal obligation** (UK GDPR Article 6 (1)(c)), to **perform a public task** (public health functions under the NHS Act 2006) (UK GDPR Article 6 (1)(e)), for the **provision of health or social care** (UK GDPR Article 9 (2)(h)) and for **Public Health Functions** under Regulation 3 for the Health Service Control of Patient Information) Regulations 2002 (UK GDPR Article 9(2)(i)).

For further information please see [Flu vaccines and the COVID-19 response - NHSX](#) and [NHS England » National COVID-19 and Flu Vaccination Programmes](#)

Covid-19 Testing

Your information will be processed for any PCR testing accessed via the Trust and for the asymptomatic test programme using the Lateral Flow Test kits and LAMP tests. This will be processed for the provision of the test and for any subsequent contact tracing. The information will be shared with your Line Manager, Divisional Manager, HR and the Infection Prevention and Control Team to help reduce the risk of potential outbreaks.

Testing information will also be shared Public Health England as part of the ongoing national response to the COVID-19 pandemic. This is a statutory requirement as COVID-19 is a notifiable disease.

A more detailed Privacy Notice is available for LAMP testing [here](#).

This processing is necessary to **perform a public task** (UK GDPR Article 6 (1)(e)). The processing is necessary for the **provision of health or social care** (UK GDPR Article 9 (2)(h)) and for **Public Health Functions** under Regulation 3 for the Health Service Control of Patient Information) Regulations 2002 (UK GDPR Article 9(2)(i)).

Covid-19 Risk Assessments

Information will be used to carry out work place risk assessments for staff, including vulnerable groups. Line Managers will also carry out an enhanced risk assessment process for any staff members that have not had a risk assessment and where our records show that neither a vaccine or Lateral Flow Tests (LFT) have been recorded. Risk assessments are necessary to ensure we work safely, protect people and to meet our health and safety obligations.

This processing is necessary for **compliance with a legal obligation** (UK GDPR Article 6(1)(c)). This processing is necessary to **carry out employment obligations and rights** (UK GDPR Article 9 (2)(b)) and the processing is necessary for **public health** (UK GDPR Article 9(2)(i)).

Foundation Trust Membership

We will also use your information to administer staff membership to the Foundation Trust. Staff will automatically become members but can opt out of membership by contacting the Foundation Trust Membership Office on telephone number: 01482 389132 or email: hnf-tr.members@nhs.net

We will use this information to communicate with you about things that are happening in the Trust. This also includes you receiving our membership magazine, inviting you to member's events or meetings and informing you about our Governor elections.

We will only process this information when it is in the **legitimate interests** of the Trust (UK GDPR Article 6(1)(f)). Please see [Foundation Trust Membership Privacy Notice](#)

ShinyMind App

Your staff contact details (Name, Employee ID number and NHSmail address) will be used by Cynergy UK to provide you with a log-in for the ShinyMind App. The App is a wellbeing and resilience resource designed to support all members of staff in the organisation. We do understand that not everyone will want to be part of the App, so if you would like to opt out, please email us at hnf-tr.proud@nhs.net.

Our legal basis for processing this information is the **legitimate interests** of the Trust (UK GDPR Article 6(1)(f)). On signing up to the App, you will need to agree with the ShinyMind privacy policy.

Electronic Communications

For specific information on how NHSmail uses your personal data please see [NHSmail Transparency Information](#)

The Trust will monitor the use of electronic communications such as e-mail or internet use following the procedure set down in the Electronic Communications and Internet Acceptable Use Procedure. The Trust will respect an employee's privacy and autonomy in business communications. However, in certain circumstances it may sometimes be

necessary to access and record an employee's business communications for the Trust's business purposes which include the following:-

- Providing evidence of business transactions
- Making sure the Trust's business procedures, policies and contract are adhered to.
- Complying with any legal obligations (including Subject Access Requests)
- Training and monitoring standards of service.
- Preventing or detecting unauthorised use of the Trust's communication system or criminal activities.
- Preventing, detecting or investigating NHS Fraud or Corruption.
- Maintaining the effective operation of the Trust's communication systems.
- Business continuity

We only process this information when it is in the **legitimate interests** of the Trust (UK GDPR Article 6(1)(f)).

National Fraud Initiative

The Trust participates in the Cabinet Office's National Fraud Initiative: a data matching exercise to assist in the prevention and detection of fraud. We are required to provide particular sets of data to the Minister for the Cabinet Office for matching for each exercise.

This is **necessary to comply with a legal obligation (UK GDPR Art 6(1)(c))** and does not require consent under the data protection legislation. For further information, please see the [full text fair processing notice](#).

WHEN DO WE SHARE YOUR INFORMATION

Personal data about you may be shared with other Trust departments in order to administer your employment. We will seek your express permission before your personal data is shared with third parties unless we are required to share information about you by law. Wherever possible we will tell you what information is being disclosed, to whom and why. Whenever we can we shall remove details which identify you.

Use of Third Party Companies

To enable effect staff administration, the Trust may share your information with external companies to process your data on our behalf in order to comply with our obligations as an employer. Examples include:

Employee Records. The information you provide during the course of your employment (including the recruitment process) will be held on the NHS Electronic Staff Record (ESR). The system is managed by the NHS Business Services Authority. See [NHS Electronic Staff Record \(ESR\) Privacy Notice](#) for further information.

Staff Survey: Data shared for the purposes of the staff survey. This is a national requirement and all data is shared securely with a contracted provider.

Occupational Health Services: Data may be shared for the purposes of occupational medical assessments and support services. This will be with your agreement.

Care Record Guarantee

At the request of the patient, the Trust will provide a list of all staff who have accessed

their health records and when they did so. The Trust will also inform the patient if their records have been deliberately accessed without permission or good reason. This is required by the NHS Care Record Guarantee.

The Access to Health Record Policy will be followed when releasing audit trail information to the patient. The full names of staff detailed on the record will be provided unless it is likely to cause serious harm to the member of staff's physical or mental health or condition. This decision will be made by the "Appropriate Health Professional" as defined by Schedule 3, Part 2, Section 2(1) of Data Protection Act 2018.

Access to health records will be monitored in line with the [Information Governance IT Forensic Investigation and Confidentiality Audit Procedures](#)

Freedom of information requests

Under the Freedom of Information Act 2000 anyone, employee or member of the public alike, has a right to ask to see this type of information. In line with being open and publicly accountable, the Trust has a legal duty to make available such information if requested to do so.

As an employee of the Trust there will be certain information about you which is of a non-private nature. This could be details of your job title and your position within the organisation, the amount of expenses you incurred whilst on official business, or perhaps details of opinions given or decisions made in meetings which are minuted and attributed to you.

Each request would be assessed individually and if appropriate you will be consulted before any information is given. In some circumstances information can be withheld but we would need to be able to justify the reason for this. If for instance we are asked to confirm the work address of a member of staff who has been physically threatened, then the decision would be made not to give out that information. However you should be aware that where the information requested is about you acting in a work or official capacity then the decision would normally be made to disclose it.

YOUR RIGHTS

Under the General Data Protection Regulation you have the right to:

- The right to be informed – we tell you what we do with your information. We do this through notices like this, and notices on our Intranet
- The right to object – you have the right to object to how we process your information. Your objection will be considered in relation to your particular situation, we will stop processing unless there is a legitimate reason for us to continue processing.
- The right to rectification - we will correct any personal information that is inaccurate or rectify any data that is incomplete.
- The right to restrict processing – we will temporarily restrict processing your data, whilst we check the information, if you query the accuracy of it. We will also restrict processing (if you raise an objection to how we process your data) whilst we consider your objection.
- The right of access – you can ask for copies of information we hold about you. This is called a subject access request.

If you would like a copy of your staff records or Occupational Health Records see [Data Protection Procedure for Employment Records](#)

You can also access information via ESR Self Service

<https://intranet.humber.nhs.uk/directorates/esr-self-service.htm>

DATA STORAGE AND RETENTION

We will create and maintain employment files for each staff member. The information will be stored confidentially and only used for purposes directly relevant to your employment.

We will retain this information in accordance with the Records Management Code of Practice for Health and Social Care Records 2016, please see: [Records Management Code of Practice for Health and Social Care Records 2016](#)

CONTACTS

If you have any issues about how your data is handled, you can contact the Trust's Data Protection Officer:

Lisa Davies, Head of Information Governance and Legal Services, Mary Seacole Building, Willerby Hill, Willerby, HU16 6ED or Tel: 01482 477854.

Information Governance Team: Email: hnf-tr.IGTeam@nhs.net or Tel: 01482 477854.

Additionally, you have the right to raise a complaint with the Information Commissioner's Office (ICO), Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Helpline: 0303 123 1113 or report online at: <https://ico.org.uk/concerns/handling/>

Last updated : May 2021.