

Privacy Notice – Trust Staff Information and Records

COVID-19 Update: Due to urgent public health operational responses in dealing with the emerging Covid-19 pandemic the Trust may need to share your information with trusted partners or process your data for purposes that are not specifically highlighted within this Privacy Notice at the time but which are essential to our COVID-19 response. Where we need to do this we will ensure that your data is kept safe and secure at all times, will limit the data used and will only do so where this is deemed appropriate to the emerging health emergency and where we have an established legal basis to do so.

For more information, please see our supplementary **COVID-19 Privacy Notice** [here](#)

Privacy information for COVID-19 virus testing for NHS workers and their household members can be found [here](#)

North Tees and Hartlepool NHS Foundation Trust (the “TRUST”) is a ‘Data Controller’ under Data Protection Legislation, including but not limited to the General Data Protection Regulation (Regulation (EU) 2016/679) (the “GDPR”), and the Data Protection Act 2018.

This means we are legally responsible for ensuring that all personal data that we hold and use is done so in a way that meets the current and future data protection principles. We must also notify the Information Commissioner about all of our data processing activity.

This Trust is registered to the Information Commissioner’s Office; **registration number Z1142263**

During the course of its employment activities, North Tees and Hartlepool NHS Foundation Trust (NTHFT) collects stores and processes personal information about prospective, current and former staff.

This Privacy Notice includes data collected and used for applicants, employees (and former employees), workers (including agency, casual and contracted staff), volunteers, trainees and those carrying out work experience.

We recognise the need to treat staff personal and sensitive data in a fair and lawful manner. No personal information held by us will be processed unless the requirements for fair and lawful processing can be met.

What types of personal data do we handle?

In order to carry out our activities and obligations as an employer we handle data in relation to:

- Personal details such as name, address, telephone number(s), email, date of birth;
- Personal demographics (including gender, race, ethnicity, sexual orientation, religion);
- Medical information including physical health or mental condition (occupational health information);
- Emergency contact(s), e.g. next of kin details;
- Education and training;
- Biometric data (including facial recognition used for clock in/out systems);

Privacy Notice – Trust Staff Information and Records

- Employment details (including job role, place of work, references and proof of eligibility to work in the UK, references and security checks);
- Information relating to the validity of an individual's passport;
- Membership of professional bodies and/or trade union(s);
- Bank details, e.g. in order to pay your salary;
- Pension details;
- Offences (including alleged offences), criminal proceedings, outcomes and sentences;
- Employment tribunal applications, complaints, accidents and incident details;
- Visual images, e.g. photographs on staff notice boards or CCTV monitoring;
- Records of Trust systems use (e.g. audit trails of system access);
- Supervision and appraisal documentation, including performance information for the purposes of capability reviews;
- Records of staff vaccination status for flu, Covid-19 and other applicable vaccinations (both of staff who have been vaccinated and those who have not);
- Records of staff Covid-19 testing results and status;
- Sickness absence and annual leave details;
- Information relating to staff who are members of the Trust's car parking scheme, including car registration number and entry/exit times. This information is issued to the Trust by Parking Eye and North Tees and Hartlepool Solutions.
- Information regarding conflicts of interest and secondary employment;
- Information relating to investigations of a disciplinary nature, which includes witness statements, notes of meetings, outcomes of the investigations and sanctions (where relevant);
- Information relating to health and safety;
- Information relating to you and your family where required for response to Pandemic planning and response

What is the purpose of processing data?

We only collect and use your information for the lawful purposes of administering the business of the Trust. These purposes include:

- To undertake obligations and exercising specific rights in the field of employment, social security and social protection law;
- Staff administration and management (including payroll and performance)
- Pensions administration;
- Administration of salary sacrifice schemes;
- Business management, modelling and planning;
- Accounting and Auditing;
- Accounts and records;
- Crime prevention and prosecution of offenders;
- Education;
- Completion of local and national staff surveys;
- Verification of identity, including passports and processing of DBS (disclosure and barring service) applications;
- Health administration and services;
- To provide health protection services relevant to your employment;
- To support local and national flu and Covid-19 vaccination and testing programmes – for example we may share your vaccination / testing status that we store with your line

Privacy Notice – Trust Staff Information and Records

manager, human resources and/or occupational health colleagues to contact you to provide relevant and appropriate health promotion, support and employee services where it is proportionate and relevant to do so or where we have a wider legal basis to do so for public interest or public health purposes;

- The provision and management of employee services (including occupational health, employee support and wellbeing services);
- To allow the Trust to contact you to provide management, administration and employee services;
- To support the work of the Joint Forum;
- To publish declarations of conflicts of interest on the register available on Trust website;
- To keep images to identify you either as part of the various security access systems, including CCTV, or as part of an overall briefing system for senior managers;
- We may use footage from CCTV for training purposes but would pixelate individuals so they are non-identifiable;
- To allow the Trust policies to be implemented and acted upon when appropriate;
- Information and databank administration;
- Sharing and matching of personal information for national fraud initiative;
- To comply with the Transfer of Undertakings Protection of Employment (TUPE) Regulations;
- To facilitate the streamlining of NHS services;
- To comply with Public Health emergencies and requirements as your employer to protect you and your family

The Trust may use your information in order to gather evidence for disciplinary and other staff processes. The use of this information will always be proportionate in relation to the evidence being sought.

What is our legal basis for processing?

We have a legal basis to collect and process this data as part of your contract of employment (either permanent or temporary) or as part of our recruitment processes, following data protection and employment legislation.

We do not rely on consent to use your information as a 'legal basis for processing' for the above purposes. We rely on specific provisions made under Article 6 and 9 of the General Data Protection (GDPR) regulations.

These are:

For the use of Personal Data

- Article 6(1)(e) - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.

For the use of Special Category Data (sensitive data)

Where we process special categories data for employment or safeguarding purposes the condition used is:

Privacy Notice – Trust Staff Information and Records

- Article 9(2)(b) - processing is necessary for the purpose of carrying out the obligations and exercising specific rights in the field of employment and social security and social protection law;

Where we process special categories data to assess the working capacity and provide occupational and health services to our employees the condition used is:

- Article 9(2)(h) – processing is necessary for the purpose of preventive or occupational medicine

Additional purposes and legal basis are used as applicable:

Vaccination and Testing Programmes – Where we collect and process information relating to staffs vaccination and testing status and provide follow up, support and health promotion – the Trust rely on the legal basis set out above, however the Trust where deemed appropriate may also rely on Article 6(1)(d) - where processing is necessary in order to protect the vital interests of either the staff or another person; and Article 9(2)(g) or Article 9(2)(h) where deemed processing is necessary in the Public Interest or for public health purposes.

ESR Streamlining – NHS organisations in utilising the streamlining programme (see sharing section), may have a legitimate interest in the effective and efficient transfer of employees from one NHS organisation to another by the transfer of certain personal data. If this processing falls outside the performance of our tasks in a public interest Article 6(1)(e), our legal basis in this instance would be that we process under Article 6(1)(f) Legitimate Interests.

Trust Marketing - To keep images that appear in Trust or other publications or websites to market and promote the Trust – the legal basis for this is per Article 6 (a) – Consent. You should be aware that once you have approved your image to appear in a publication we may not be able to completely retrieve this image if you change your mind about its use. Your image may appear again later unless you specifically indicate otherwise.

Communication of critical messages - In order to utilise all communication methods available, key corporate messages may be sent via SMS to staff personal mobile phones with your consent. If you wish to receive these key messages on your personal phone, you would need to add your number to the Trust's telephone book, which can be accessed via the main SharePoint site under the tab 'Phonebook'. You can easily 'opt in' or 'out' by adding/deleting your mobile number from the field named '**SMS Opt in Service**' at any time. Once your number is added here this will only be visible to yourself and a small number of staff who administer the system, it will not be visible to other staff across the Trust. Only messages deemed critical or of high importance will be shared in this way and we will endeavour only to send these messages during daytime / working hours.– if you 'opt in' to this service the legal basis we will use to process your data this way is per Article 6 (a) – Consent.

Legal Proceedings - We may also process personal data for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings), for the purpose of obtaining legal advice, or for the purpose of establishing, exercising or defending legal rights. Where we process personal data for these purposes, the legal basis for doing so is:

- Article 6(1)(e) – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
- Article 6(1)(c) – processing is necessary for compliance with a legal obligation to which

Privacy Notice – Trust Staff Information and Records

- the controller is subject; or
- Article 6(1)(f) – processing is necessary for the purposes of legitimate interests pursued by the controller.

Where we process special categories of personal data for these purposes, the legal basis for doing so is:

- Article 9(2)(f) – processing is necessary for the establishment, exercise or defence of legal claims; or
- Article 9(2)(g) – processing is necessary for reasons of substantial public interest.

Disclosure and Barring Service (DBS) – Information relating to criminal convictions and offences are processed in accordance with GDPR Article 10 provisions and only where required, for example under the provisions of the Safeguarding Vulnerable Groups Act 2006 as the basis for Disclosure and Barring Service (DBS) checks and other processing of such data.

The legal basis for any other use will be explained at the point of collection within the relevant statutory provisions.

How do we keep information safe?

We are committed to keeping your information secure and have operational policies and procedures in place to protect your information whether it is in a hardcopy or electronic format.

All of the Information Systems used by our Trust are implemented with robust information security safeguards to protect the confidentiality, integrity and availability of your personal information. The security controls adopted by the Trust are influenced by a number of sources including the 10 National Data Guardian Standards and guidelines produced by NHS Digital and other Government standards.

Your information is stored in both paper (personnel files held by Human Resources and/or your line manager) and also electronically on ESR. Other temporary files may be created as a result of investigations, disciplinary investigations, occupational health reviews or complaints but these will usually be kept separately from the personnel file or destroyed in line with the agreed destruction criteria. If a sanction is applied, it will be noted on the personnel file.

Everyone working for the NHS is subject to the Common Law Duty of Confidence. Information provided in confidence will only be used for the purposes advised and consented to, unless it is required or permitted by the law. Our staff are trained to handle your information correctly and protect your confidentiality and privacy.

We aim to maintain high standards, adopt best practice for our record keeping and regularly check and report on how we are doing. Your information is never collected or sold for direct marketing purposes.

We also protect your information by following data protection laws:

- General Data Protection Regulation (GDPR)
- Data Protection Act (DPA) 2018

The GDPR and DPA are the laws that primarily determine how we can use your personal data.

Privacy Notice – Trust Staff Information and Records

However, there are other laws that are followed if we need to process your information:

- The Human Rights Act 1998
- Freedom of Information Act 2000
- Computer Misuse Act 1998
- Audit Commission Act 1998
- Regulation of Investigatory Powers Act 2000

If you post or send offensive, inappropriate or objectionable content anywhere on www.nth.nhs.uk or on the Trust's Facebook, Twitter or any other Trust social media page, or otherwise engage in any disruptive behaviour we may use whatever information is available to us, about you, to stop such behaviour.

Do we process information overseas?

On occasions your data may be processed outside the UK, in most circumstances it will remain within the European Economic Area (EEA). The same protection would be applied as if processed within this country. If your data is transferred outside the EEA we are required to comply with the Data Protection Act, and ensure there is adequate protection is in place ensuring that appropriate and suitable safeguards and binding contractual clauses are in place.

Data collected will not be sent to countries where the Laws do not protect your privacy to the same extent as the law in the UK, unless rigorous checks on the security and confidentiality of that data are carried out in line with legal requirements.

How long do we retain information?

Employment data will be retained in compliance with the Records Management Code of Practice for Health and Social Care 2016 which details retention periods for employment records. This is available on the NHS Digital website at <https://digital.nhs.uk/information-governance-aiance> or on the Trust's SharePoint site.

We keep CCTV images for 28 days from the day of capture.

Who do we share information with and why?

There are a number of reasons why we share information. This can be due to:

- Our obligations to comply with legislation;
- Our duty to comply with any Court Orders which may be imposed;

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 or where we have another legal basis to share.

We will not routinely share any information about you to anyone outside the Trust without your consent. However, there are circumstances where we must or can share information about you owing to a legal/statutory obligation.

Privacy Notice – Trust Staff Information and Records

We may obtain and share personal information with a wide variety of other bodies, which may include, but is not limited to:

- Her Majesty's Revenue and Customs (HMRC);
- Department for Work and Pensions (DWP);
- Disclosure and Barring Service (DBS);
- Home Office;
- Child Support Agency;
- Regulatory bodies, e.g. NMC, GMC;
- Law enforcement agencies including the Police and the Serious Organised Crime Agency;
- NHS Business Services Authority - National NHS Electronic Staff Record (ESR) system;
- NHS England, NHS Improvement and NHS Digital.

We may also use the information we hold about you to detect and prevent crime or fraud and where appropriate and where we have a legal basis share with relevant agencies. We may also share this information with other bodies that inspect and manage public funds.

To enable effective staff administration North Tees and Hartlepool NHS Foundation Trust may use external companies to process your data on our behalf in order to comply with our obligations as an employer. Our partner data processors are legally bound to respect your confidentiality, and comply with our security operating procedures (see *Data Processors*).

Electronic Staff Record (ESR)- 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 effectively manage the workforce leading to improved efficiency and improved patient safety.

Streamlining - Streamlining is the process by which certain personal data is transferred from one NHS organisation to another when your employment transfers. NHS organisations have a legitimate interest in processing your data in this way in establishing the employment of a suitable workforce. The streamlining programme is a data sharing arrangement which is aimed at improving efficiencies within the NHS both to make costs savings for Trusts but also to save you time when your employment transfers. In accepting employment with the Trust, you accept that relevant personal data for the purpose will be transferred under the streamlining programme if your employment transfers to another NHS organisation.

NHS Staff Survey – The Trust may share limited identifiable data with approved data processors contracted to undertake national and local NHS staff surveys on its behalf. The completion of the survey is voluntary and no identifiable data is shared back to the Trust on the responses given.

Disclosure and Barring checks/information (DBS) - Given the nature of our organisation, DBS requirements may apply to our employees. 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 your normal duties. In all cases, we carry out the checks in line with the applicable law. For clinical and other regulated roles, the DBS checks will be repeated periodically during the course of employment in line with Trust processes.

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,

Privacy Notice – Trust Staff Information and Records

technical, and organisational security measures designed to secure your personal data against accidental loss and unauthorized access, use, alteration, or disclosure.

DBS information will be deleted once the applicable checks have been completed subject to any exceptional circumstances and/or to comply with particular laws or regulations. DBS information will typically be retained for a maximum of 6 months, although the outcome of any check will remain on the employee's record.

Data Processors - as a Trust we have entered into contracts with other organisations to provide services for us. These range from software companies who provide our Electronic Staff Records and online survey tools to contractors who provide specialist services that help provide a better service to you as an employee. These contractors may hold and process data including staff information set out in this privacy notice on our behalf.

These contractors are known as '**Data Processors**' and subject to the same legal rules and conditions for keeping personal information confidential and secure as the Trust is. We are responsible for making sure that staff in those organisations are appropriately trained and that procedures are in place to keep information secure and protect privacy. These conditions are written into legally binding contracts, which we will enforce if our standards of information security are not met and confidentiality is breached.

COVID-19 Statement – Data Processors

Data processors (as defined above) may be used for Covid-19 staff data processing. The Trust may need to appoint approved data processors in order to process data collected from you in regards to Covid-19 testing, Covid-19 results and the Covid-19 services we provide or offer to you. Data processors will only be appointed where it is necessary, the data they process will be limited to only that required for the specific purpose and will be held by the processor for the minimum amount of time required for that purpose in response to the Covid-19 pandemic response. For further information, please contact the Trust DPO.

What are your rights as an individual?

Data Protection law gives individuals rights in respect of the personal information that we hold about you and these apply in circumstances where the relevant conditions are met.

These rights are, the right:

1. To be informed why, where and how we use your information.
2. To ask for access to your information.
3. To ask for your information to be corrected if it is inaccurate or incomplete.
4. To ask for your information to be deleted or removed where there is no need for us to continue processing it.
5. To ask us to restrict the use of your information.
6. To ask us to 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)
9. To lodge a complaint to the supervisory authority – Information Commissioners Office (ICO)

Privacy Notice – Trust Staff Information and Records

More Information about Your Rights

There are additional restrictions to the above rights of individuals and these are listed in GDPR Article 23 and can be obtained from the Trust on request.

You retain the right to seek remedy from a court under section 167 of the Data Protection Act 2018 where you feel these rights have not been appropriately applied.

For further information on your rights please visit the ICO website www.ico.org.uk or contact the Trust Data Protection Officer.

How can I access my information?

You can request access to the information that the Trust holds about you and you should do this by approaching your line manager in the first instance. They will provide you with guidance on the Trust's processes.

Your request, once agreed with you, will be completed within one calendar month. However, if your records are extensive we may take longer to process your request but will inform you from the outset, and in any case within one calendar month. To submit a formal request, please contact:

Human Resources Department-Subject Access Requests
Floor 3, North Wing
University Hospital of North Tees
Hardwick Road
Stockton-On-Tees
TS19 8PE

As well as receiving a copy of the information that the Trust holds and processes, you are also entitled to the following:

- To be told whether any personal data is being processed.
- Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people.
- Given a copy of the personal data together with its source (where this is available).

COVID-19 Statement – Access to Information

Your request for information may be delayed due to urgent operational responses to dealing with Public Health priorities. We apologise for any inconvenience this may cause, we do remain committed to responding to your request and will respond as soon as we are able. Should our response to your request breach the statutory timeframe and you remain unhappy with our response you have the right to complain to the Information Commissioners Office.

Privacy Notice – Trust Staff Information and Records

What if I have concerns about how the Trust is handling my data?

The **Data Protection Officer (DPO)** is the person to contact if you would like to know more about how we use your information, if you require information in any accessible format or language, you wish to make a complaint or if (for any reason) you do not wish to have your information used in any of the ways described and to exercise your rights.

The DPO can be contacted at:

Post:

Data Protection Officer
Information Governance Department
University Hospital of North Tees
Hardwick Road
Stockton-On-Tees
TS19 8PE

Telephone:

01642 624470
(Monday and Friday, 9am to 5pm)

Email: nth-tr.infogov@nhs.net

Should you wish to lodge a formal complaint about the use of your information you can also contact your line manager or the Human Resources Department either by phone (see internal telephone directory), in person or in writing:

Human Resources Department
Floor 3, North Wing
University Hospital of North Tees
Hardwick Road
Stockton-On-Tees
TS19 8PE

Whilst we ask that, you allow us time to address your concerns and that you come to us first, you also have the right to lodge a complaint with the supervisory authority directly if you are not content with the outcome of your confidentiality and data protection complaint and/or concern raised with the Trust.

You can contact the Information Commissioners Office (ICO) at:

Post:

Information Commissioner's Office (ICO)
Wycliffe House, Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone:

0303 123 1113 (Local Rate) or +44 1625
545 745 (outside UK)

Online: www.ico.org.uk

Privacy Notice – Trust Staff Information and Records

Further Information

Should you have any further queries on the uses of your information, please speak to our Data Protection Officer, your line manager or to Human Resources.

Changes

It is important to point out that we may amend this Privacy Notice from time to time to ensure that you can stay in control of your data and you should check regularly for any changes.

Date Last Updated 14/04/2021