UHNM NHS Trust - Staff Privacy Notice

This privacy notice is for all current, former or prospective staff of UHNM NHS Trust.

If you are a patient, carer or relative, you should see our patient privacy notice. The patient privacy notice will also apply, in addition to the staff privacy notice, where staff are involved in health initiatives, including COVID-19 research.

1. Introduction

University Hospitals of North Midlands NHS Trust (also known as "the Trust") is registered as a data controller with the Information Commissioner's Office (ICO) as part of the Data Protection Act 2018; our notification number is Z6476085. We're committed to collecting, storing and processing personal information in line with UK Data Protection Law and the UK General Data Protection Regulation (GDPR).

This privacy notice tells you what to expect when the Trust collects personal information about you. This notice aims to inform you about the types of data we collect, why we collect it, and how we ensure its security.

The Trust will keep your records as defined within the following policies:

Policy No.	UHNM Policy Title
G09	Management, Protection and Disclosure of Employment Related Information
G16	Standards of Business Conduct
DSP10	Data Security, Protection and Confidentiality
DSP15	Information Asset Management
DSP16	Information Lifecycle and Records Management
DSP17	Access to Personal Information (Subject Access Request)
DSP18	Overarching Data Security and Protection [DSP] Policy
IT01	Corporate Policy for Information Security
IT02	Personal Information Security and Acceptable Use

And all other UHNM policies referencing the use of staff information, e.g. our people (HR) policies.

All UHNM's policy documents are available to staff on the Trust's intranet

For the purposes of this staff privacy notice, the term 'staff' includes current, former and prospective (in alpha order):

- Applicants
- Apprentices
- Bank and Agency workers
- Employees
- External Learners (who require an ESR account because they require access to our IT systems but may not be an actual employee, although working in the organisation in some capacity)
- Honorary Contract holder e.g. Clinical academics

- Independent Contractors
- Medical Observers contract holder (formerly known as a clinical attachment)
- Non-executive directors
- Secondees
- Student placements
- Trainees
- Volunteers
- Work experience placements

However, the information we will process about you will vary depending on your specific role and personal circumstances.

We reserve the right to update this privacy notice at any time, and we'll notify you with a new privacy notice if we make any substantial updates. From time to time, we may also let you know about the processing of your personal information in other ways.

2. Types of information we collect

Personal information (also called personal data)

This is information that identifies you, like your name or contact details or an IP address or your medical records.

It's important that the personal information we hold about you is accurate and up to date. Please let us know if your personal information changes during your working relationship with us.

If any changes are required, please let us know by contacting your line manager in the first instance or by emailing the Trust's ESR Department (but please note UHNM's ESR team do not work weekends or bank holidays).

If any changes are required to your details, please log into your ESR account and update your details – this will then need authorising within ESR by your line manager or you can contact the Trust's ESR Department via esrsupportuhnm@uhnm.nhs.uk (but please note UHNM's ESR team do not work weekends or bank holidays). Alternatively, there are several user guides available here: ESR FAQ's | University Hospitals of North Midlands NHS Trust (UHNM Intranet → MyUHNM →MyHR → ESR → ESR FAQ's). Please also note you cannot change your DOB or National insurance number in ESR. If these need correcting in ESR these must be changed via your line manager and the payroll team.

Special category personal information

Some of the information we collect is special category data, or likely to be more sensitive data, which can include your:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership / affiliation
- Genetic data
- Biometric data
- Sexual orientation
- Gender identity
- Health (physical and mental health) - either declared by you or obtained from health checks, occupational health referrals and reports, return to work meeting notes after sickness absence, health management questionnaires or fit notes, for example, Statement of Fitness for Work from your GP or hospital.

- Information you have provided regarding Protected Characteristics as defined by the Equality Act for the purpose of equal opportunities monitoring. This may be extended to include other protected characteristics. For example, this may include self-declarations of any form of disability.
- Details of any DSE, access needs, risk assessments or reasonable adjustments.
- Accident records if you have an accident at work.

Criminal conviction data is not held as a special category but requires extra safeguards to be put in place.

Extra safeguards are applied to special category information, and we must be able to demonstrate a legitimate reason to hold and use it.

3. When we collect information about you

If you apply for a job

When you apply for a position with the Trust via **trac**, or **NHS Jobs**, you will give us relevant information about you which includes:

- your name
- date of birth
- personal contact details
- details of your skills, qualifications, employment history, experience, and professional membership (if relevant), and training history
- referee details

If you are invited to interview

During recruitment and selection, we will collect additional information like:

- correspondence, interview notes, and results of any tests you're asked to complete as part of the selection process
- copies of qualifications and certificates
- pre-employment checks, including referees and disclosure and barring checks (DBS)
- For certain roles, we are required to seek information about past criminal convictions, working with children or vulnerable adults, and/or your fitness to practise in certain regulated professions.
- your nationality and immigration status, to confirm your eligibility to work in the UK
- your national insurance number, tax and bank details
- details of your pension
- remuneration, including salary and entitlement to benefits
- trade union membership
- ethnicity, gender, health, religion or sexual orientation
- medical history relevant to your employment, including physical health, mental health and absence history
- we may check publicly available information, like your social media presence

If you become an employee

If you are employed by us, we may collect additional information like:

- your image, for security and ID badge
- next of kin information
- education and training history

- appraisal and performance reviews
- security and audit data when you use Trust IT equipment and systems, including the use of NHS smart cards, and when you use your own computer or device to access Trust systems including device identifiers and IP addresses
- your performance, sickness absence and other work-related matters
- NHS number
- CCTV recordings when you're on Trust premises
- personal data recorded as a normal part of your work activity
- data relating to employee relations, like complaints, or grievances (resolution cases) or conduct / disciplinary proceedings (with internal or external investigation officers and/or case managers)
- your car details for car parking permit purposes
- details of any secondary employment, conflict of interest declarations or gift declarations

If you are an external learner

If you are an external learner, not directly employed by the Trust, you will provide us with relevant information about you, like:

- title
- full name
- date of birth
- national insurance number
- relevant email address

4. Why we collect your personal information

The Trust doesn't always need your consent to collect and use your personal data. The Trust can process it without your consent if we have a valid reason. These reasons are known in law as a 'lawful basis'; and there are **six** lawful bases organisations can use.

It is therefore important for you to know the various lawful bases that we rely on under data protection law for the processing of your personal data (i.e. as set out in Article 6 of the UK GDPR). To be able to process your data lawfully, we must rely on a specific lawful basis, depending on the main reason why we need the data. No single basis is 'better' or more important than the others. Below is an explanation of these lawful bases and when they might be used.

4.1 Giving us your consent to process your data for a specific purpose

We may sometimes ask for your consent to do something that involves use of your personal data. We will do this where no other lawful basis applies and where it makes sense to give you the highest level of control over how your data is used by us. For this reason, we will not ask for your consent very often where your data is being processed for employment reasons because one of the other lawful bases listed below will often be more appropriate.

However, you would be asked to specifically consent to the processing of your data if, for example, we wished to use your image in marketing or PR materials; wished to send you marketing, or to process your data where we cannot rely on one of the below bases.

Consent should be clearly given, informed and recorded.

4.2 Necessary for the Trust to perform (enter into and manage) a contract with you

We process your data to carry out the contract of employment or worker agreement we have with you, or to enter into it in the first place – for example, ensure you can work in the UK, pay you a salary and keep records of disciplinary, complaint or grievance (resolution) proceedings.

4.3 Necessary for the Trust to comply with a legal obligation

We process data about you under this legal basis when we need to comply with UK legislation, such as in the areas of employment for tax and National Insurance purposes (HMRC), UK Visas and Immigration requirements (UKVI) purposes or to comply with the Equality Act, or laws around health and safety in the workplace. At times of a service provision change, this may include the transfer of Employee Liability Information under the Transfer of Undertakings (Protections of Employment) Regulations amended 2014 [TUPE].

It should be noted that this does not include contractual obligations.

4.4 Necessary for the purposes of the Trust's (or a third party's) legitimate interests

Sometimes we will process your data because we have identified a 'legitimate interest' in doing so. The legitimate interests we identify are determined through an assessment made by weighing our requirements against the impact of the processing on you. This is done to make sure that our legitimate interests will never override your right to privacy and the freedoms that require the protection of your personal data.

Examples of when we will process your data in our legitimate interests

- Recruitment and selection purposes
- Providing you with a Trust photo ID card / badges
- Providing you with personalised access to buildings, facilities, library services and car parking
- Providing you with UHNM IT account, access to a UHNM email account, and give you, IT applications, resources / equipment and network services such as Wi-Fi.
- Monitoring use of IT services to ensure adherence to the Trust's IT Policies
- Managing and monitoring network and systems access including cyber security and forensic requirements
- Managing employee relations (human resources) process, like sick pay, managing absence, parental leave, and workforce planning
- Managing employee relations cases, investigations and outcomes
- Maintaining staff records, including payroll, benefits, corporate travel and other reimbursable expenses, development and training, absence monitoring, performance appraisal, conduct, management progress, disciplinary and grievance (resolution) process and complaints, pensions administration, and other general admin and people (HR) services related processes
- Monitoring equal opportunities
- Providing you with access to training and development services
- Providing you with access to the online benefits portal to enhance reward offering and visibility
- Enabling effective communications to you about Trust security or operations and to keep you informed and involved with what's happening at the Trust, including news and events
- Contacting those people you have named to be notified in the event of an emergency.
- Maintaining contact with former staff
- Operating and keep a record of employee performance and related processes to plan for career development, succession planning and workforce management purposes.
- Using staff information to conduct strategic analysis, modelling and forecasting to help the Trust plan ahead.
- Service quality monitoring

- Analysing the effectiveness of a service that we provide, such as our annual NHS National staff survey. This analysis is carried out at an aggregate level so that you are not identifiable from the data.
- Maintaining patient health records, in line with the Trust's clinical records keeping standards
- Managing safe environments and fitness to work
- Occupational health and wellbeing services
- Ensuring that we can keep Trust sites safe and secure, and taking measures to prevent and detect crime. This involves capturing images of you in our CCTV system. More information about how your data is processed within the CCTV system can be found in Trust Policy EF20 - Closed Circuit Television (CCTV); and includes a privacy notice for CCTV. The government's updated Surveillance Camera Code of Practice came into effect from 12 January 2022. The CCTV policy is readily available on the Trust's intranet page. Alternatively, you can contact the Trust's Fire Safety and Security team for further information.
- Fraud prevention
- With the Trust's insurance brokers and insurers and related third parties, e.g. lawyers and loss adjustors for the purpose of risk mitigation, securing insurance cover, maintaining and administering that cover and processing any claims that may arise as a result.
- Operating and managing our own internal business intelligence data and analytics services, via a secure ESR to UHNM data connection. As described further below:

  <u>Internal Data Warehouse – Operated by UHNM Trust</u>

  - Some of your personal information from ESR will be securely transferred, on a daily basis, to our own internal database, known as the ESR General Data Warehouse. The ESR Information Asset Owner will operate as the gateway person, who will decide on who can or who cannot access this data source, and the level of data access which is permitted on a per user basis.
  - This data source will be used internally for the creation of dashboards and to integrate access to our internal IT systems, as the single source of truth, regarding who should and who should not access certain clinical and none-clinical systems. This central source of truth will also allow authorised individuals to access certain personal information to generate the reports they require to ensure the security and confidentiality of our IT systems.

4.5 Necessary to protect your vital interests or those of another person

On very rare occasions, we may need to access or share your information to protect your life or that of another person, for example in an emergency situation where we cannot gain your consent or to do so could endanger life. We will only rely on vital interests in extremely limited circumstances when no other legal basis is available.

4.6 Necessary for the purpose of performing a public task in the public interest

For the purpose of securing insurance cover for the general protection of the Trust and its staff, maintaining and administering that cover and processing any claims that may arise as a result.

We will use your information to administer your employment and associated functions. Your information may be shared between relevant colleagues who need the information to carry out their duties, like your line manager or People Directorate (HR) teams.

We maintain electronic and paper records that relate to your recruitment and employment. This information is held by the People (HR) Directorate and locally, with your line manager. All paper files are securely stored, and only relevant staff will be able to access this information.

Electronic information is accessed on a need-to-know basis, using the Trust's ESR and other systems. Some information may be held on the Trust's secure electronic drives, where access is only granted to appropriate individuals.

Where we process sensitive personal or special categories of data about you, we will ensure this is done only where one of the following conditions applies:

- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller, or the data subject, in the field of employment and social security and social protection law
- processing is necessary for the purposes of preventive or occupational health, assessment of the working capacity of the employee, or the provision of health or social care

If you require further information about the legal basis for any specific aspect of processing, please email the Trust's Data Security and Protection Department.

5. Sharing your data with third parties

The General Data Protection Regulation (GDPR) sets strict rules on the sharing and transfer of personal data to protect individuals' privacy rights.

In certain circumstances, we may share your data with third parties for legal or business purposes. Be assured that such sharing is conducted securely, and stringent measures are in place to protect your data during external sharing.

We may disclose personal and sensitive information to a variety of recipients when:

- there's a legal obligation to share
- it's necessary for the performance of your employment contract
- you have consented to the sharing

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 disclosed to those agencies and bodies who have a need to know, when there is a lawful basis to do so.

There are a number of circumstances where we must or can share information about you to comply with or manage:

- Disciplinary/investigation processes, including referrals to professional bodies, e.g. the Nursing and Midwifery Council or the General Medical Council
- Legislative and/or statutory requirements
- National mandatory reporting requirements
- Court orders which may have been imposed on us
- NHS counter-fraud requirements. Including the National Fraud Initiative (NFI)
- Requests for information from the police and other law enforcement agencies for the prevention and detection of crime, and/or fraud if the crime is of a serious nature.

To comply with our obligations as an employer and to provide efficient staff administration the Trust may share your data with (to) very specific third-party organisations for clearly identified purposes. Your personal data may be shared where there is a legitimate reason to do so and this is appropriate to your role and responsibilities, and recipients may include:

- Our employees, agents and contractors where there is a valid reason for them receiving the information; this includes our Payroll and Pensions service provider and those involved in salary sacrifice schemes.
- Current, past or potential employers of our staff to provide or obtain references.

- NHS Business Services Authority
- Professional and regulatory bodies in relation service reviews and the confirmation of conduct, including complaints, job descriptions and information provided as part of the recruitment, selection and redeployment processes
- UK Visas and Immigration (UKVI) which is part of the Home Office (the government's department responsible for immigration, security and law and order)
- The Disclosure and Barring Service (DBS) and DBS Update Service where we require a DBS check for certain roles
- Education, training and professional development providers
- Professional and regulatory bodies in relation Medical Revalidation, appraisal and support
- Government departments and agencies where we have a statutory obligation to provide information, like HMRC and the Department of Health
- Third parties who work with us to provide staff car parking services
- Third parties who work with us to provide staff support services and wellbeing services, like staff counselling
- Third parties who work with us to provide Occupational Health services
- Third parties who work with us to provide services in respect to Employee Relations casework
- Third parties who host employee data in the cloud (i.e. third-party software systems such as those used for employee management, absence management, recruitment, e-rostering, job-planning, coaching and leadership development etc)
- Survey organisations for example for the NHS annual National Staff Survey.
- Organisations in respect to supporting our Equality, Diversity and Inclusion staff networks and organisational objectives (e.g. To support our Stonewall submission in relation to LGBTQ+.)
- Crime prevention or detection agencies, like the police and security organisations
- Parliamentary and Health Service Ombudsman
- Internal and external auditors
- Courts and tribunals
- Our solicitors, legal advisors or counsel
- Trade union and staff associations (e.g. union subscription details in order to process salary deductions for union membership for which the employee will have given their consent).
- Relatives or guardians of an employee
- Under the FOI Act and Trust policy (DSP08) it may be necessary to release the names of Band 7's and above if requested. For further information, please refer to Policy DSP 08 - Freedom of Information / Section 4 Roles and responsibilities / including the sub-section on 'Release of Trust Employee name and details'.

We are required by law to protect the public funds we administer. Every year, the NHS is required to participate in the National Fraud Initiative (NFI) to assist in the prevention and detection of fraud. As part of this, we provide payroll information for data matching. Data matching involves comparing sets of data, such as payroll or benefits records of an organisation, against other records held by the same or another organisation. Find out more from the government's (Cabinet Office) NFI Privacy Notice or by contacting our Local Counter Fraud Specialist.

What protections are in place?

Where data is shared with third parties there is always a local contract/agreement or national contract/agreement between the provider and the Trust. A senior manager will have been identified to act as a lead person for each contract/agreement with responsibility for ensuring that your information is managed in a fair and lawful manner.

The terms of our contracts with third parties include obligations on them in relation to what personal information they can process and what they can do with that information. All our third-party service providers, professional advisers and other entities are required to take appropriate security measures to protect your personal information. We do not permit our third-party service providers to use your personal information for their own purposes – they may only process your personal information for specified purposes and in accordance with our instructions.

The list of third-party organisations will change, and processes are in place to ensure that these organisations are recorded.

Additional information about the following third parties:

NHS Business Service Authority (NHSBSA)

- The Trust also shares employee records information with the NHS Business Services Authority, which acts as a data processor for the Trust. The NHSBSA is an arm's length body of the Department of Health and Social Care.

- The information 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. It's stored on the national NHS Electronic Staff Record (ESR) system.

Electronic Staff Record (ESR)

- When you start your employment with the Trust, your personal data will be uploaded into the ESR system. IBM, who provide ESR, and its partners as service providers will be responsible for maintaining the system. This means that they may occasionally need to access your staff record, but only to ensure that the ESR works correctly.

- Where this happens, access will be limited and is only to allow any problems with the computer system to be investigated and fixed as necessary. IBM and its partners will not have the right to use this data for their own purposes, and contracts are in place with the Department of Health to ensure that the data is protected and that they only act on appropriate instructions.

- IBM and the ESR Central Team may access anonymised data about transactions on the ESR system to support the development and optimal use of the system.

Data Warehouse (external) – Operated and Controlled by IBM

- Some of your personal information from ESR will be transferred to a separate database, known as the Data Warehouse. This will be used by various Government and other bodies to meet their central and strategic reporting requirements. It will allow them to access certain personal information to generate the reports that they need and are entitled to.

- The Data Warehouse is intended to provide an efficient way of sharing information. Organisations currently granted access to the Data Warehouse are:

    - NHS England *1
    - NHS Employers
    - Deaneries
    - Department of Health
    - Welsh Government
    - NHS Wales Shared Services Partnership
    - Care Quality Commission

  *1 Please note:
    - Monitor was merged with the NHS Trust Development Authority (TDA), to form NHS Improvement (NHSI) on 1 April 2016.
    - The Health and Care Act 2022 created a single NHS organisation comprising what was previously Monitor and NHS Trust Development Authority (TDA), known as NHS Improvement. From 1st July 20202, NHS Improvement merged with NHS England (and

the two organisations within NHSI, Monitor and the NHS Trust Development Authority, no longer exist, and they are all now legally part of one NHS England).
    - As of 1 July 2022, a number of the processes and functions formerly undertaken by Monitor and the NHS Trust Development Authority transferred to NHS England.
    - From 01 February 2023 NHS Digital merged with NHS England
    - From 01 April 2023 Health Education England merged with NHS England

- The Government may allow further organisations to have access in the future and therefore an exhaustive list cannot be provided, however any organisation having access to your data will have a legal justification for access.

Staff Support and Counselling Service

- When you contact the Trust's external Staff Support and Counselling Service provider, they may record your contact details, and information about the issues you have raised and about any advice or support you have been given or referred to.

- This information is recorded to provide advice and to manage the service, including any future contact with you. Information about the matters raised will be kept separate from information that identifies you and may be used to analyse and improve the service.

- The information will be kept confidential, and access will only be available to authorised Staff Support and Counselling staff. Information which identifies you will not be shared with any other person without your consent unless this is necessary for legal and regulatory purposes.

- The legal basis for processing is our legitimate interest in providing a confidential advice and support service for the welfare of our staff.

NHS flu and COVID-19 vaccination programmes

- The Trust provides data on all staff to NHS Digital as required by the Secretary of State for Health exercising the public health functions under section 2 of The National Health Services Act 2006. This includes:
    - name
    - address
    - employee number
    - date of birth
    - gender

- The purpose is to administer and implement the NHS National Immunisation Vaccination Service (NIVS) (flu and COVID-19) immunisation programmes for NHS staff. The implementation of this service delivers a centralised data capture tool for clinical teams delivering the seasonal flu and COVID-19 immunisation and is an essential component of NHS England's response to the COVID-19 pandemic. Particulars of staff receiving immunisation are also provided to NIVS as part of the program. For further information see the NHS England Privacy Notices. Where staff have received COVID-19 immunisation elsewhere, the Trust may receive information about this from NIVS or the National Immunisation Management System (NIMS) used by GPs.

- Staff immunisation status is recorded on the Trust's Occupational Health service provider's portal (which currently has no interface with the NHS Electronic Service Record (ESR)) or Trust agency worker checklist and may be shared with managers and supervisors for the purpose of service planning and assessing suitability for employment, having regard to any requirement to be vaccinated when employed in a CQC regulated activity. Immunisation status may also be shared with other healthcare providers for that purpose. The lawful basis for processing immunisation status is:

- necessary for the performance of the employment contract with respect to any requirement to be vaccinated when employed in a CQC regulated activity
- necessary for compliance with the legal obligation in R17 of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 to maintain such records as are necessary to be kept in relation to persons employed in the carrying on of a regulated activity

- Information may be shared between providers of regulated services for the purposes of the legitimate interests of both parties in complying with the above requirements. All processing of immunisation status falls within Art 9 (2)(h) UK GDPR – necessary for the management of health or social care systems and services.

NHS National Staff Survey contracted service provider

- Data is securely shared, for the purposes of the annual NHS National Staff Survey, with the contracted survey provider, for all eligible substantive employees and any bank only people who have worked in the six-month period, prior to the commencement of the National Staff Survey.

Other NHS organisations (also known as NHS streaming)

- To streamline staff movement, we may share your information if you accept an offer with another NHS organisation, or your employment transfers or is seconded to another NHS organisation. This may also include the sharing of information via the NHS Digital Staff Passport.

- The following information may be shared if there is a legitimate business interests of the two organisations to do so:
  - personal data to verify who you are, like your name, date of birth, address, NI Number
  - employment information to allow for correct pay and annual leave and sickness entitlements, like your position, salary, and dates of any sickness
  - training compliance and 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.

Other processors

- The Trust uses specialist processors for tasks like:
  - workforce planning and analytics
  - case investigation and or case management (e.g. an employee relations case investigation undertaken by external Investigating Officer)

- This will be carried out using a contractor compliant with Article 28 of the GDPR, and with appropriate guarantees of confidentiality.

- Please note the following in respect to situations when the Trust engages an external investigating officer for an employee relations case, where the Case Manager is employed by the Trust:
  - ICO guidance on distinguishing between data controllers and processors is complex. You need to consider the personal data and the processing activity that is taking place and consider who is determining the purposes and the manner of that specific processing.
  - An employee of the Trust, who is acting within the scope of their duties as Case Manager, is acting as an agent of the data controller.

- The external Investigating Officer is acting as an ‘independent data controller’. It is commonly the case for a data controller to allow its processor discretion over how the processing takes place using its own expertise; therefore, they will be acting as a controller in their own right for that element of their processing.
- Under our Trust policy and procedures for a formal investigation, the Case Manager will specify the terms of reference for the investigation and provide this to the appointed Investigating Officer along with the relevant documentation already gathered.
- The Terms of Reference for the investigation should in effect provide the brief which specifies the purpose and framework under which the investigation is to be undertaken and reporting requirements. The Case Manager leaves it to the Investigating Officer to determine their approach to collating and reviewing relevant information and evidence, interview methods and presentation of the findings and conclusions.
- The Investigating Officer is processing personal data on the Trust’s behalf, but it is also determining the information that is collected (what to ask the Trust’s employees and/or ex-employees) and the manner in which the processing (the investigation) will be carried out. The external Investigating Officer has the freedom to decide such matters as which individuals to select for interview, what form the interview should take, what information to collect from the complainant and witnesses and how to present the results. This means the external Investigator is a joint controller with the Trust regarding the processing of personal data to carry out the Investigation, even though the Trust retains overall control of the data because it commissions the investigation and determines the purpose the data will be used for.
- The Trust has a legitimate reason for providing relevant documents to the Investigating Officer for the purpose of the investigation.

6. Conflicts of interest

All staff on consultant contracts, those at Agenda for Change bands 8a and above, or equivalent contracts, and Authorised Signatories are required to complete a declaration of interest return on an annual basis, including where staff have nothing to declare. All staff at this level who have completed this will have their declarations of interest disclosed on the Trust website. Those staff at this level who fail to complete a declaration of interest will have their names published on the Trust website as not submitting a declaration. Further information is available in the Trust’s Policy G16 - Standards of Business Conduct.

All data is processed in line with GDPR 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” based on NHS England contract requirements for publishing declarations of interest.

7. How long do we keep your data for?

As a principle, information about you will not be kept for longer than it is needed for the purpose it was collected.

The Trust has records retention policy which documents for how long different information is required. As the retention policy indicates, we need to keep different data for differing periods of time. If you have any queries regarding how long we keep your data that are not answered in the policy, please email the Trust’s Data Security and Protection Department.

When it is no longer required in line with its retention period, personal information is securely and permanently destroyed.

8. Your rights in relation to the way we process your data

As an individual whose data we process (a data subject), you have certain rights in relation to the processing. When it comes to personal data held about you by the Trust, you have the right to:

- request access / obtain your personal data for reuse
- request the correction of inaccurate or incomplete information, subject to certain safeguards
- request that your information is deleted or removed where there is no need, no legitimate grounds for us to continue processing it, and when the retention time has passed
- ask that we restrict the use of your information in certain way, based on personal circumstances
- withdraw your consent for the collection, processing and transfer of personal information for a specific purpose, where we have relied on that consent as our basis for processing your data.
- to object to certain processing of your personal data i.e. how your information is used
- to challenge automated decision making
- to lodge a complaint with the ICO

Making a complaint

If you have any concerns about the way that we have handled your personal data, please either email the Data, Security & Protection team using DSPuhnm@uhnm.nhs.uk , or email your concerns to My Employee Relations, as we would like to have the opportunity to resolve your concerns.

If we can't resolve your concern, you have the right to lodge a complaint with the Information Commissioner's Office (an independent body set up to advise on information rights for the UK) about the way in which we process your personal data.

9. Your responsibilities for your personal data

Please ensure you inform us if your personal information changes while you are working with us as it is important that the personal information that we hold about you is accurate and current.

Certain information must be provided so that we can enter into a contract with you (e.g. your contact details, right to work in the UK and payment details). You also have some obligations under your contract to provide certain information to us, e.g. to report absences. Without this information, we may not be able to carry out the rights and obligations efficiently that arise as a result of the employment relationship.

In addition, you may have to provide us with information so that you can exercise your statutory rights, e.g. parental leave. If you fail to provide the necessary information, this may mean you are unable to exercise your statutory rights.

You also have responsibilities in relation to personal information, and must comply with our Trust's Data Security and Protection policies, which can be found on our intranet, which includes:

- taking appropriate steps to protect the security of personal information
- being careful about who personal information is disclosed to
- protecting your communications and devices
- reporting data breaches
- following other business processes in relation to the handling of third-party personal information
- being up to date with your statutory and mandatory training requirements for information governance and data security and protection.

10. How to access your personal data

If you require copies of personal information held by the Trust, speak to your line manager in the first instance.

Alternatively, you can make a Subject Access Request [SAR] by emailing My Employee Relations 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.

Further information is available in our Trust Policy DSP17 Access to Personal Information (Subject Access Request - SAR)

The People Directorate (formerly known as Human Resources Directorate) have a Standard Operating Procedure in place to ensure that workforce Subject Access Requests are dealt with in accordance with ICO guidance and 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.

Information:
The Trust may refuse your request in full or in part, where there is a legal basis to refuse, and you will be informed of this.

11. More information

If you have any further questions on the uses of your information, please contact your line manager or you can email the Trust's Data Security and Protection Department, or ESR Department, or My Employee Relations.

We are committed to keeping this privacy notice updated. Regular reviews are conducted to align with any changes in data protection laws or our practices. Your privacy matters, and we strive to ensure our policies reflect latest standards.