

Privacy Notice for Staff

This is a Privacy Notice - also known as a Fair Processing Notice.

This page describes how the Trust uses and manages the information it holds about its staff, including how the information may be shared with other organisations, and how the confidentiality of staff information is maintained.

Personal data is information that relates to a living individual who can be identified from that data.

The Trust is registered with the Information Commissioner's Office as a [Data Controller Royal United Hospitals Bath Z8889967](#)

Legal Basis for Processing of Personal Data

The Trust holds personal information about its staff (including substantive staff, Bank staff and volunteers) for employment-related purposes and to allow the Trust to provide our services in an effective, safe and professional way.

The processing is necessary for the contracts that the Trust holds with its staff and in order to comply with UK employment law, as well as complying with our obligations as a care provider and public authority.

The GDPR which came into force in May 2018 will continue to operate in UK law after the UK exits the EU (European Union).

This will not affect your rights, your contract of employment or the information that is processed about you.

Please see below for further details.

To ensure that the NHS at local, regional or national level is getting the most from the public purse, workforce information is used to support the development of a Workforce plan, as part of the Strategic Workforce Planning Workstream.

This is done under 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' (please see the Strategic Workforce Programme section below).

The Trust may rely on 'legitimate interests' where the processing is deemed necessary for either your or RUH's legitimate interests or unless there is a good reason to protect an individual's personal data which overrides those legitimate interests.

This may include, but is not limited to, monitoring the use of Trust systems or apps.

How staff records may be used

The Trust shares staff information with a range of organisations or individuals for a variety of lawful purposes, including:

- Disclosure to data processors - e.g. to companies providing archive storage of personnel records under contract to the Trust
- Public disclosure under Freedom of Information - e.g. requested names or contact details of senior managers or those in public-facing roles
- Disclosure of job applicant details - e.g. to named referees for reference checks, to the Disclosure and Barring Service for criminal record checks, to named GPs for health checks, to housing agencies for staff relocation or accommodation
- Disclosure to employment agencies - e.g. in respect of agency staff
- Disclosure to banks and insurance companies - e.g. to confirm employment details in respect of loan/mortgage applications/guarantees, with individual consent
- Disclosure to professional registration organisations - e.g. in respect of fitness to practice hearings;
- Disclosure to occupational health professionals (subject to explicit consent)
- Disclosure to police or fraud investigators - e.g. in respect of investigations into incidents, allegations or enquiries, or in response to a court order

Confidential staff information is only shared with other organisations where there is a legal basis, when one of the following applies:

- When there is a statutory duty to share staff data
- When there is a statutory power to share staff data
- When the employee has given their explicit consent to the sharing

The National Fraud Initiative (NFI) is an exercise that matches electronic data within and between public and private sector bodies to prevent and detect fraud.

From 2017/18, NHS bodies were added to the mandatory list of responders.

The core datasets include payroll data.

For 2020, the Trust is required to take part in the National Flu Vaccination Programme which is led by NHS England.

Information needs to be shared as part of this programme.

If you would like to see what information is being used and the lawful basis for using it, then please see the [NHS England website: National Flu Vaccination Programme](#).

Vaccination status

During the pandemic, information about vaccination status of staff was collected and where necessary, it was stored nationally on secure approved systems. This was to support the response to Covid-19. Data Protection Impact Assessments were completed at this time.

The decision to make vaccinations a condition of employment has now been reversed and therefore the data that was being shared by RUH has stopped. The Trust will continue to maintain local records of vaccinations for our staff. This will be managed in the same way as we maintain occupational health records of staff and will be processed similar to seasonal flu vaccines data. We need to keep this data to ensure that we offer vaccines to the right people and to ensure safe care of our staff. This information will be

stored in accordance with the Records Management Code of Practice 2021 and data protection legislation.

Sharing Information held in the Electronic Staff Record

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.

In accepting employment with the Trust, you accept that the following personal data will be transferred under the streamlining programme if your employment transfers to another NHS organisation:

- Personal information such as your name, date of birth and contact details
- Recruitment information including qualifications, registrations with professional organisations, National Insurance (NI) Number, etc.
- Payroll information
- Assignment details (job role, department etc.)
- Training records

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.

Strategic Workforce Programme

Developments in health and care services are driving organisations to work even more closely together to provide the best quality care, whilst achieving the greatest value for money.

It is widely recognised that the sharing of relevant data in a timely and secure manner supports the delivery of effective care.

The Trust will support the development of a wider workforce plan, as part of the Strategic Workforce Planning Workstream, through the sharing of workforce information.

Data from organisations and providers across the whole health and social care economy within the BSW STP (Bath and North East Somerset, Swindon and Wiltshire Sustainability and Transformation Partnership) will be processed and used to establish the relationship between workforce capacity and service delivery.

This will use information held in the Electronic Staff Record (ESR) and will include data such as:

- Job role
- Division
- Directorate
- Speciality/Department
- Mid-point of job pay scale

Step into Health

The Step into Health programme supports employers in the NHS to recruit from the Armed Forces community (e.g. service leavers, spouses, dependents) by providing tailored access routes to employment and training opportunities.

As part of this work the team at NHS Employers provides tools, guidance and support to NHS organisations so they can engage with the Armed Forces community and therefore have a more representative workforce.

For more information, please see the [Step into Health Privacy Notice](#).

Culture Shift (Report and Support)

Your personal data (information which identifies you as an individual), including any sensitive personal data (e.g. special categories of personal data such as, racial or ethnic origin, physical or mental health) that you provide is handled in accordance with the Trust's Information Governance Management Policy, our Data Protection by Design and Default policy and this privacy notice. Together they provide information about how we protect your privacy.

How your data will be used

We may use the information you provide for the purpose of:

Helping us to identify the best person for you to speak to in relation to your report.

Providing the person with your contact details (if you have provided them) and some useful background information that will enable them to understand the nature of your concern or the incident you are reporting.

Where applicable, reviewing your report and taking further action if required. We will write to you to keep you informed of what we are doing.

Once we have concluded any actions we have taken, we will write to you to inform you of the outcome.

Reporting Anonymously

When reporting anonymously, we will not ask you for any personal identifiable details. Please be aware that if you disclose on an anonymous basis, the Trust will not be able to offer direct advice or take any action on the report. However, we will keep an anonymised record of your report to identify whether there have been/are

other similar reports and whether there is a pattern of behaviour or trends that should be addressed.

For us to be able to assist you fully, we encourage you to provide us with your personal details.

Disclosing your personal data

Your identity and your other personal data will be disclosed within the Trust on a need-to-know basis only. We will always seek to process the minimum amount of personal data possible for us to deal with your report. Personal data will not be disclosed to any third parties without your consent unless there are legitimate reasons requiring us to do so, for example, where the information you have provided highlights a potential risk to a person's health and safety.

Retaining your data

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. We will keep records of all reports, both anonymous and named, for 1 year from case closure on the 'Report + Support' system. We may retain some anonymised information to monitor our work in this area, but you will not be identifiable from this information.

Your data rights

You have certain rights in relation to your personal data, subject to certain conditions. These include:

- The right to access your personal data held by us.
- The right to require us to rectify any inaccurate personal data held by us about you.
- The right to require us to erase personal data held by us about you where we no longer need to use the personal data to achieve the purpose, we collected it for; or where you withdraw your consent if processed on this basis. Please note, a withdrawal of consent may prevent us from reviewing and processing a report, and/or from taking further action based upon that report
- The right to restrict our processing of personal data held by us about you, e.g., Where we no longer need to use the personal data to achieve the purpose, we collected it for, but we require the data for the purposes of dealing with legal claims.

If you have any questions, comments and requests regarding our data processing practices and your rights, please send to ruh-tr.igqueries@nhs.net

You can also find more information about how your information is processed as part of the reporting system provider's (Culture Shift) Privacy Notice [Culture Shift Report and Support](#)

Retention

Your personal data will be retained by the Trust in accordance with the retention schedule outlined in the Records Management Code of Practice 2021.

Staff access to their information

Trust employees have the right to access personal information about them held by the Trust, either to view the information in person, or to be provided with a copy.

Staff members wanting to access their employment information should contact their Human Resources representative.

Requests are normally fulfilled within 30 calendar days of receiving the request in writing.

There is no charge for this unless the request is deemed to be manifestly unfounded, excessive or repetitive.

If we determine this to be the case we will notify you of this in writing.

For employees who are also patients of the Trust, please see [Health Records Access](#)

Security

CCTV (closed circuit television) is utilised to protect the safety of our patients, staff and members of the public.

The Trust remains the data controller of this data and any disclosures to third parties such as the police, will only be done with the permission of the Trust.

To maintain privacy and dignity, recordings will not be permitted in areas of the hospital where examinations or procedures are being undertaken or if there is likely to be nudity.

Further information

For further information about this notice, or any other data protection matter please contact the Information Governance team:

Tel: 01225 826468

Email: ruh-tr.IGQueries@nhs.net

Royal United Hospitals Bath NHS Foundation Trust
Combe Park
Bath

BA1 3NG

For further guidance concerning the General Data Protection Regulation and Subject Access Requests in general, please contact:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow

Cheshire
SK9 5AF

Tel: 0303 123 1113 or 01625 545745

Or please see the [Information Commissioner's Office website](#).

Changes to our privacy notice

Any changes we may make to our privacy notice in the future will be posted on our website and on the intranet. Where appropriate we will notify you by email.

Please check back frequently to see any updates.