

Employee privacy notice

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

You should read this Notice carefully and raise any questions you may have with the operational HR team or Data Protection Officer.

Scope

In connection with your employment, the relevant data controller is **Berkshire Healthcare NHS Foundation Trust, Fitzwilliam House, Skimped Hill Lane, Bracknell, Berkshire, RG12 1BQ.**

What personal data do we collect?

Personal data means information which identifies you and relates to you as an individual. As your employer, the Trust will collect, use and store your personal data for a wide variety of reasons in connection with the employment relationship.

We have set out below the main categories of employee personal data which we process on a day-to-day basis:

- personal contact information (including your name, home address, personal telephone number(s) and personal e-mail address)*
 - business contact information (including e-mail address and telephone number)
 - job title
 - date of birth*
 - driving licence number *
 - gender
 - marital status
 - emergency contact information
 - photograph
 - documents evidencing your right to work (including information about your immigration status where relevant)*
 - bank account details*
 - documents gathered during the recruitment process (including cv, application form, references, professional memberships and qualifications, background vetting information)*
-

-
- documents maintained and updated during your employment relating to professional memberships and qualifications and statutory and mandatory training (including but not limited to professional revalidation)*
 - general employment records including details of training, disciplinary and grievance matters, benefits, holiday and other absences, along with a copy of your employment contract, performance records (including appraisals) and compensation history*
 - data evidencing your COVID-19 vaccination status* (unless your role has been identified by the Trust as not being in scope of the requirement to provide evidence of COVID-19 vaccination status)
 - information gathered through the Trust's monitoring of its IT systems, building access records and CCTV recording*
 - personal data which you otherwise voluntarily provide, for example when using your Trust e-mail account

The personal data provided by you and identified at * above is mandatory in order for us to administer the employment relationship and/or comply with statutory requirements relating to immigration, taxation and the protection of the health of vulnerable people and individual workers. Failure to provide mandatory personal data may affect our ability to accomplish the purposes stated in this Notice and potentially affect your ongoing employment.

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

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

How do we use your personal data?

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

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

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

What special categories of personal data do we process?

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

Health Information

The Trust may process information about an employee's physical or mental health in compliance with its obligations in connection with employment, in particular (i) to administer sick pay entitlements; (ii) to facilitate the assessment and provision of NHS Injury Allowance; (iii) to comply with obligations owed to disabled employees; (iv) to comply with patient care, health regulatory and health and safety obligations; and (v) to maintain a sickness absence record; (vi) to obtain Occupational Health advice and support from the Trust's external Occupational Health Service Provider; (vii) to comply with the requirements to review and retain proof of your COVID-19 vaccine status as detailed in Government guidance and pursuant to the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 as amended by the Health and Social Care Act 2008 (Regulated Activities) (Amendment) (Coronavirus) (No 2) Regulations 2022, or any subsequent legislation) and in order to protect the health of vulnerable people and individual workers.

In respect of data evidencing your COVID-19 vaccination status, a small number of designated staff in the HR and Immunisations Team will access the Cinnamon Immunisation System (if your COVID-19 vaccinations were administered by the Trust) and/or National Immunisation Management Service (NIMS) and/or National Immunisation Vaccine Service (NIVS) databases and view your COVID-19 vaccination record. The requirement to evidence COVID-19 vaccination status covers both clinical and non-clinical workers who are not directly involved in patient care but who nevertheless may have direct, face-to-face contact with patients, such as receptionists, ward clerks, porters and cleaners. Your vaccination status will also be shared with staff involved in your management, including your direct line manager, as and when required for staff and risk management.

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

Health information will typically be retained during the course of an individual's employment. Following the termination of an individual's employment, we will typically retain health information for 7 years, in line with our normal retention arrangements, subject to any exceptional circumstances and/or to comply with particular laws or regulations.

Disclosure and Barring checks/information (DBS)

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

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

For clinical and other regulated roles, 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, technical, and organisational security measures designed to secure your personal data against accidental loss and unauthorised 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.

Equal Opportunities Monitoring

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

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

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

When do we share employee personal data?

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

- Payroll providers
- Benefits providers
- Background vetting specialists
- Occupational health providers
- The Department of Health
- Any applicable regulatory body
- HMRC and/or any other applicable government body
- Accountants, lawyers and other professional advisers

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

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

For how long will my personal data be retained?

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

During the course of an individual's employment the Trust will review an individual's personnel record approximately every 24 months and any personal data which is no longer needed will be deleted.

Following the termination of an individual's employment, the Trust will typically retain data for 7 years after which the individual's entire employment file will be destroyed, subject to any exceptional circumstances and/or to comply with particular laws or regulations.

What are my rights in relation to my personal data?

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

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

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

You have a separate right of access to your personal data processed by the Trust. 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. If you wish to exercise your right of access you should set out your request in writing to your local Data Protection Officer using the details set out below.

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

Website ico.org.uk/concerns/

Call [0303 123 1113](tel:03031231113)

Email casework@ico.org.uk.

Where can i get further information?

The Trust has appointed a Data Protection Officer to oversee compliance with this Notice and to deal with any questions or concerns. The Data Protection Officer for Berkshire Healthcare is the Clinical Information Governance Manager. If you would like further information about the matters set out in this Notice, please contact the Trust's Data Protection Officer or a member of the HR Team.

The contact details for your Data Protection Officer are set out below:

Email: information.governance@berkshire.nhs.uk

Postal address:

Berkshire Healthcare NHS Foundation Trust

Fitzwilliam House

Skimped Hill Lane

Bracknell

Berkshire

RG12 1BQ

Call [01344 415600](tel:01344 415600)