

Staff Privacy Notice

In this page

How we use information about you

National Fraud Initiative

How long we keep your record

Your information rights

Accessing your record

Contact the Information Governance team

How we use information about you

As an employee of the Trust, your personal information is processed (created, stored and transmitted) in a variety of paper and electronic formats by the Trust in accordance with the provisions of current data protection law. The lawful basis for this is the [General Data Protection Regulation \(GDPR\)](#) Article 6, paragraph 1(b) - processing is necessary for the performance of a contract to which the data subject is a party.

Sensitive personal data, as defined by legislation, includes that relating to ethnic origin, disability, religious belief, sexual orientation and gender identity. You will have been asked to provide personal sensitive information during the recruitment process. The Trust is obliged to seek this information from staff but it is not compulsory for staff to provide responses. Access to and the sharing of this information is controlled very carefully. When reporting on personal sensitive information only aggregate data is presented so that an individual's data is protected.

There is a legal obligation on the Trust, as employer, to provide information regarding the commission of offences, or alleged commission of any offence, or any proceedings for any offence committed, the disposal of proceedings, or the sentence of any courts of any such proceedings.

[See GDPR Article 10](#)

The Trust also receives requests made by applicants, under the Freedom of Information Act (FOIA) 2000 and the Environmental Information Regulation (EIR) 2004. The applicant may request information which may involve your

personal data. We will need to, in most cases, consider whether or not disclosure would contravene the data protection principle (a) - lawfulness, fairness and transparency. We have a legal obligation to process any personal data, we hold, when considering whether or not the information should be disclosed pursuant to these requests under the FOIA 2000 and the EIR 2004.

The data that we use is held securely and confidentially. Your data is used to ensure that you are paid correctly and that we have the correct contact address/telephone number so that we can communicate with you if required, either in an emergency or as part of a routine matter.

Your personal information is used for a number of purposes, including:

- recruitment
- Disclosure and Barring (DBS) checks
- internal reviews
- absence monitoring
- equality and diversity monitoring.

Access to the information is restricted to staff who require access to it in order to carry out their contractual duties.

We may use external service providers to help manage employee services e.g.:

- UHB Payroll
- GoodShape
- Disclosure and Barring Service
- TRAC recruitment online management tool
- our staff survey provider.

This list is not exhaustive and staff will be notified about any new use of their data. When we contract with an external supplier we ensure that your data will be held securely.

Your anonymised data is also used to provide management information. Internal management information reporting is an important management tool for all large organisations to meet statutory reporting requirements, to monitor its policy and performance, and to develop equality aims and objectives and provide a better understanding of our diverse Trust workforce.

As well as reporting internally, aggregated, anonymous data from the Trust is used nationally to help facilitate benchmarking, and assist in the planning of the National Health Service (NHS).

National Fraud Initiative

The Trust is required **by law** to protect the public funds it administers. It may share information provided to it with other bodies responsible for auditing or administering public funds in order to prevent and detect **fraud**.

The Cabinet Office conducts data matching exercises to assist in the prevention and detection of fraud. This is one of the ways in which the Minister for the Cabinet Office takes responsibility within government for public sector efficiency and reform.

Data matching involves comparing sets of data, such as the payroll or benefits records of a body, against other records held by the same or another body to see how far they match.

The data is usually personal information. The data matching allows potentially fraudulent claims and payments to be identified. Where a match is found it may indicate that there is an inconsistency that requires further investigation.

No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out.

Data matching by the National Fraud Initiative is subject to a [Code of Practice](#).

The processing of data by the Cabinet Office in a data matching exercise is carried out with statutory authority under its powers in **Part 6 of the Local Audit and Accountability Act 2014**. It does not require the consent of the individuals concerned under data protection legislation or the GDPR.

We participate in the Cabinet Office's [National Fraud Initiative - see guidance here](#). We are required to submit [different categories of data](#) to the NFI on a regular basis.

For further details regarding how your personal data will be used, including your rights, please read the [National Fraud Initiative Privacy Notice](#).

How long we keep your record

Your record will be kept for six years after you have left the Trust, after which it will be summarised, the full record confidentially destroyed, and the summary kept for six years or until your 75th birthday, whichever is the longer. This is in line with the [Records Management Code of Practice for Health and Social Care 2016](#).

Your information rights

- You have the right to know how we will use your personal information

- You have the right to see your record
- You have the right to object to us making use of your information other than for managing your employment
- You can ask us to change or restrict the way we use your information and we have to agree if possible
- You have the right to ask for the information we hold about you to be corrected or erased if it is incorrect

If you object to how we are using your information, or wish us to restrict, erase or correct it, or would like further information about how we use your information and your rights, please contact our Information Governance team.

Accessing your record (a Subject Access Request)

While you are employed by the Trust you may ask to see your employment record by contacting the Information Governance team.

Your record will be prepared for you and a qualified member of staff will talk you through the content. Your right to see some information may be limited - for example, if it includes details about other people.

To access your record after you leave Trust employment, or if you want copies of your record, please also contact the Information Governance team.

Contact the Information Governance team

- Email: information.governance@ouh.nhs.uk
- Tel: 01865 226912