Staff Privacy Notice

During the course of its employment activities, Leeds Community Healthcare Trust collects, stores and processes personal information about prospective, current and former staff (including agency, casual and contracted staff), volunteers, trainees and those carrying out work experience.

We recognise the need to treat staff Personal and Special Category Data in a fair and lawful manner.

This Privacy Notice should be read in conjunction with our HR policies.

Contents

[Who we are 1](#_Toc148447088)

[What types of personal data do we handle? 2](#_Toc148447089)

[What are the purposes of processing your personal data? 3](#_Toc148447090)

[Legal Basis 3](#_Toc148447091)

[Sharing your information 6](#_Toc148447092)

[How long is your personal data kept for? 8](#_Toc148447093)

[Your rights in relation to personal data we hold 8](#_Toc148447094)

[Requesting access to your Personal Data 9](#_Toc148447095)

[Where can I get more information? 9](#_Toc148447096)

[Complaints 9](#_Toc148447097)

# Who we are

Leeds Community Healthcare NHS is a data controller under the UK General Data Protection Regulation and will collect, store and use Personal Data about you to manage your employment.

Our registered address is

White Rose Office Park, Building 3, Leeds LS11 0LT

Information Commissioner’s Office (ICO) registration:  Z258777X

# What types of personal data do we handle?

In order to carry out our activities and obligations as an employer we a wide variety of types of data including (but not limited to):

* Personal demographics (including gender, race, ethnicity, sexual orientation, religion)
* Your position, role, contract terms, grade, salary, benefits, entitlements and working hours
* Contact details such as names, addresses, telephone numbers and emergency contact(s)
* Employment records (including professional membership, references and proof of eligibility to work in the UK and security checks)
* Bank details
* Pension details
* Medical information including physical health or mental condition (including occupational health information)
* Information relating to health and safety
* Trade union membership
* Offences (including alleged offences), criminal proceedings, outcomes and sentences
* Employment Tribunal applications, complaints, accidents and incident details
* Details of disciplinary procedures
* Details regarding professional development and appraisals
* Vehicle registration and insurance details
* Application details, including copies of passports, driving licence and driving history, right to work documents, visas and other immigration data.
* IT related information such as emails addresses and Active Directory details
* Staff photographs and other visual identifiers such as CCTV

Our members of staff are provided with training to ensure that your information is handled correctly and that the confidentiality and privacy of this information is protected.

We will always hold the minimum required amount of data for our purposes.

Your information is never collected or sold for direct marketing purposes.

Your information may be processed outside of the UK, although this would only happen in limited circumstances and in such cases an appropriate risk assessment will have been carried out.

# What are the purposes of processing 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 some of the main purposes for which employee personal data is processed:

* Staff administration and management (including payroll and performance)
* Pensions administration
* Business management and planning
* Accounting and Auditing
* Accounts and records
* Crime prevention and prosecution of offenders
* Education
* Health administration and services
* Information and databank administration
* Sharing and matching of personal information for national fraud initiative
* Public Health
* Security and estate management

# Legal Basis

The Trust’s legal bases for most processing of personal data under the UK GDPR are as follows:

For Personal Data

* Article 6.1 (b): “processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract”.

This legal basis is used to support your employment contract, and our joint obligations and responsibilities in regard to this.

* 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”

This legal basis is used for areas where we have a particular public duty.

For Special Category Data

* Article 9.2 (b): “processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment”

This legal basis is used to support your employment contract, and our joint obligations and responsibilities in regard to this.

* Article 9.2 (h): “processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services”

This legal basis is used to support processing for the purposes of managing the Trust’s activities.

For criminal conviction information

* Article 10: “Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by domestic law providing for appropriate safeguards for the rights and freedoms of data subjects.”

This is supported by Schedule 1, Part 1 of the Data Protection Act 2018: “processing in connection with employment, health and research - Processing necessary for the purposes of performing or exercising obligations or rights of the controller or the data subject under employment law, social security law or the law relating to social protection.”

This legal basis is used where we may obtain data via the Disclosure and Barring Service or for any process of justice you may be involved in.

Other Legal bases may apply in particular situations, including:

Article 6.1 (a): “the data subject has given consent to the processing of his or her personal data for one or more specific purposes”- this legal basis would be used for specific situations where we might require a positive opt in for a specific situation.

Article 6.1 (c): “processing is necessary for compliance with a legal obligation to which the controller is subject”- this legal basis would be used in instances where would be compelled to provide information, such as a court order or a statutory request.

Article 6.1 (d): “processing is necessary in order to protect the vital interests of the data subject or of another natural person”- this legal basis would be used when we needed to share personal information, such as if we think there may be threat to someone’s health or safety.

Article 9.2 (a): “The data subject has given explicit consent to the processing of those personal data” - this legal basis would be used in situations where would need your specific consent to share Special Category Data.

Article 9.2 (c) “processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent”- this legal basis would used where we needed to share Special Category Data if we think there may be threat to someone’s health or safety and it is not practicable to get consent.

Article 9.2 (g): “processing is necessary for reasons of substantial public interest, on the basis of domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject”- this legal basis would be used when supported by a specific public interest, set out in paragraphs 6 to 28 of Schedule 1 of the DPA 2018

Article 9.2 (i): “processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices,”- this legal basis would be used in situations such as disease outbreaks, or where we needed to share data to ensure that our services would be clinically safe.

Sharing your information

As above, there are a number of reasons why we might share information.

Any disclosures of personal data are always made on a 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.

Some of the reasons for sharing your personal data and also with whom they are shared with are:

**Third Party Companies**

To enable effective staff administration, Leeds Community Healthcare Trust may share your information with external companies to process your data on our behalf in order to comply with our obligations as an employer and support the effective management of the Trust.

**Employee Records; Contracts Administration (NHS Business Services Authority)**

The information which 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, held on the national NHS Electronic Staff Record (ESR) system.

**Prevention and Detection of Crime and Fraud**

We may use the information we hold about you to detect and prevent crime or fraud. We may also share this information with other bodies that inspect and manage public funds.

We will not routinely disclose any information about you without your express permission. However, there are circumstances where we must or can share information about you owing to a legal/statutory obligation.

**National Fraud Initiative**

Leeds Community Healthcare 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, or where undertaking a public function, in order to prevent and detect fraud.

The Cabinet Office is responsible for carrying out data matching exercises.

Data matching involves comparing computer records held by one body against other computer records held by the same or another body to see how far they match. This is usually personal information. Computerised data matching allows potentially fraudulent claims and payments to be identified. Where a match is found it may indicate that there is an inconsistency which requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out.

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](http://www.legislation.gov.uk/ukpga/2014/2/part/6). It does not require the consent of the individuals concerned under data protection legislation or the GDPR.

Data matching by the Cabinet Office is subject to a [**Code of Practice**](https://www.gov.uk/government/publications/fair-processing-national-fraud-initiative/fair-processing-level-3-full-text).

View further information on the [**Cabinet Office’s legal powers and the reasons why it matches particular information**](https://eu-west-1.protection.sophos.com/?d=www.gov.uk&u=aHR0cHM6Ly93d3cuZ292LnVrL2dvdmVybm1lbnQvcHVibGljYXRpb25zL2ZhaXItcHJvY2Vzc2luZy1uYXRpb25hbC1mcmF1ZC1pbml0aWF0aXZlL2ZhaXItcHJvY2Vzc2luZy1sZXZlbC0zLWZ1bGwtdGV4dA==&e=YmVyaWMuZGF3c29uQHRpYWEuY28udWs=&t=djJVNjFGNXNYNTZxeVEySnRwNTZzZkM2NlQrOVA2RmhwMDNFcmJvMTlLWT0=&h=e59bf08327314d3ea594930f10ca5d35).

For further information on this data matching exercise contact the Trusts Counter Fraud Specialist Nikki Cooper; mobile 07872 988939 or email: nikki.cooper1@nhs.net

# How long is your personal data kept for?

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.

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.

# Your rights in relation to personal data we hold

The Data Protection law gives individuals rights in respect of the personal information that we hold about you.  These are:

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)

Please note that the rights available to you are specific to the legal basis used to process the data, so not all rights are available under all circumstances.

# Requesting access to your Personal Data

Under Data Protection legislation, this is known as a ‘Subject Access Request’ and all employees have the right to make such a request to the Trust to obtain access to the information that we hold about you. Any such request must be dealt with within one-calendar month of the request being made; except where numerous requests are made or the request being made is complex, in which case the deadline can be extended by a further two months.

# Where can I get more information?

Should you have any further queries on the uses of your information, please speak to the Human Resources Department or our Data Protection Officer – Steve Creighton on DPO.LCH@nhs.net or 0113 220 8572.

# Complaints

You have the right to complain to the Information Commissioner if you are not happy with any aspect of Leeds Community Healthcare’s processing of your personal data or believe that we are not meeting our responsibilities as a data controller. We would, however, appreciate the chance to deal with your concerns before you approach the ICO, so please contact the Data Protection Officer at first instance.

The contact details for the Data Protection Officer are:

Steve Creighton

White Rose Office Park, Building 3, Leeds LS11 0LT

dpo.lch@nhs.net

The contact details for the Information Commissioner are:

Information Commissioner’s Office Wycliffe House Water Lane, Wilmslow SK9 5AF

[Information Commissioner's Office Website.](https://ico.org.uk/)