THE DUDLEY GROUP NHS FOUNDATION TRUST

General Data Protection Regulation (GDPR) Privacy Notice

We issue this privacy notice in the interests of transparency over how we use ("**process**") the personal data that we collect from job applicants/employees ("**you**"). It does not form part of your contract of employment and may be amended from time to time.

Personal data for these purposes means any information relating to an identified or identifiable person.

"**Sensitive personal data**" or "**Special Category Data"**, means personal data consisting of information as to -

- the racial or ethnic origin of the individual,
- their political opinions,
- their religious or philosophical beliefs,
- their membership of a trade union,
- their physical or mental health or condition,
- their sexual life,
- the commission or alleged commission by them of any offence,
- any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings,
- genetic data; and
- biometric data where processed to uniquely identify a person (for example a photo in an electronic passport)

Data Controller

For data protection purposes the "**data controller**" means the person or organisation who determines the purposes for which and the manner in which any personal data are processed.

The Data Controller is **The Dudley Group NHS Foundation Trust (The Trust).**
The Data Protection Officer is **Sharon Williams** who can be contacted at sharonwilliams2@nhs.net

The kind of information we hold about you

We will collect, store and use the following categories of personal data about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Marital status and dependants.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date.
- Location of employment or workplace.
- Copy of driving license.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Performance information.
- Disciplinary and grievance information.
- CCTV footage and other information obtained through electronic means such as swipe card records.
- Information about your use of our information and communications systems.
- Photographs.

We may from time to time also collect, store and use the following sensitive personal data:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership.
- Information about your health, including any medical condition, health and sickness records.

- Genetic information and biometric data.
- Information about criminal convictions and offences.

Purpose of processing the data

It is necessary for us to process personal data of both job applicants and employees for the following reasons:

1. We will need the information in order to identify the individual for the purposes of recruitment;
2. We will need to maintain that information for the general purposes of the ongoing employment relationship including performing the employment contract and maintaining the health and safety of individuals on our premises.

Some examples of the specific situations in which we will use your personal data are:

- making decisions about your recruitment or appointment determining the terms on which you work for us;
- checking you are legally entitled to work in the UK;
- paying you and, if you are an employee, deducting tax and National Insurance contributions;
- providing benefits to you;
- liaising with your pension provider;
- business management and planning, including accounting and auditing;
- conducting performance reviews, managing performance and determining performance requirements;
- making decisions about salary reviews and pay;
- assessing qualifications for a particular job or task, including decisions about promotions;
- gathering evidence for possible grievance or disciplinary hearings;
- making decisions about your continued employment or engagement;
- making arrangements for the termination of our working relationship;
- education, training and development requirements;
- dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work;
- ascertaining your fitness to work;
- managing sickness absence;
- complying with health and safety obligations;
- to prevent fraud;
- to ensure compliance with our IT policies;
- to ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution;
- equal opportunities monitoring.

Our legal basis for processing personal data of applicants and staff is that:

1. Processing the personal data is necessary for the purpose of carrying out the employment contract or to take steps to enter into an employment contract;
2. Processing is necessary to comply with a legal obligation (for example we are obliged under employment law to include in a written statement of employment terms the identity of the parties to the employment contract; and to ensure your health and safety); and/or
3. Processing the data is necessary for the purposes of our "**legitimate interests**" as the data controller (except where such interests are overridden by the interests, rights or freedoms of the individual).
4. Processing is necessary for the performance of the task carried out in the public interest or in the exercise of official authority vested in the controller.
5. Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment or management of health or social care systems and services on the basis of union or member state law or a contract with a health professionals.

Our "legitimate interests" for these purposes are:

1. the need to process data on applicants and staff for the purposes of assessing suitability for employment and then carrying out the employment contract;
2. the need to gather data for the purposes of safeguarding the health and safety of job applicants and employees;

3. the need to transfer employee data intra-group for administrative purposes; and
4. the need to process employee data for the purposes of ensuring network and information security.

We may from time to time need to process sensitive personal data of the kind described above.

In that case we will either obtain the explicit consent of the individual to the processing of such data or we may consider the processing of that data as being necessary for carrying out our obligations as an employer. That will be assessed on a case by case basis.

There is no strict statutory or contractual requirement for you to provide data to us but if you do not provide at least that data that is necessary for us to assess suitability for employment and then to conduct the employment relationship then it will not practically be possible for us to employ you.

Recipients of personal data

Your personal data may be received by the following categories of people:

1. Our HR department;
2. In the case of job applicants, the interviewer and prospective manager;
3. Any individual authorised by us to maintain personnel files;
4. Our professional advisers
5. Insurance companies and any other third party necessary to comply with any legal disclosure; and
6. Appropriate external regulators and authorities (such as HMRC and HSE)

We do not envisage that your data would be transferred to a country outside the EEA. If we perceive the need to do that we would discuss that with you and explain the legal basis for the transfer of the data at that stage.

Use of Third Party Companies

To enable effective staff administration The Dudley Group NHS Foundation Trust will share your information with external companies to process your data on our behalf in order to comply with our obligations as an employer. This includes payroll and pensions processing and occupational health services as outlined below:

1. Payroll and Pensions: Data shared for purposes of payroll and pensions provision (NHS Pensions).
2. Occupational Health Services: Data shared for purposes of occupational health medical assessments and support services (Remploy and BHSF).
3. Employee Records; 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.
4. Staff Survey: Data shared for purposes of a national requirement for NHS staff to be surveyed. Data will be shared securely with the contracted provider.
5. Membership Engagement Services Limited: As a member of staff you are automatically enrolled into the Foundation Trust membership base with the option to 'opt out'. The trust's legal basis for processing is that it's necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. We share your information in order that they can host the membership database. It is not given to any other third party unless we are legally required to do so.

What information do we receive from other sources?

Information may be provided about you from a number of sources during your recruitment and on-going employment with the Trust including:

- Disclosure and Barring Service disclosures, where applicable, which will tell the organisation about any criminal convictions you may have
- Referees providing confidential information about your suitability to the role
- Inter Authority Transfer (IAT) – Information held by your previous NHS employer
- Information from HM Revenue and Customs (HMRC) relating to your pay and employment
- Information about your right to work and visa applications
- Pension Information when transferring within the NHS
- Information from your manager and HR team relating to your performance, sickness absence and other work related matters
- Confirmation of your registration with a professional body

Duration of storage of personal data

We will keep personal data for no longer than is strictly necessary, having regard to the original purpose for which the data was processed. In some cases we will be legally obliged to keep your data for a set period.

Examples are below:

- Income tax and NI returns, income tax records and correspondence with HMRC: We are obliged to keep these records for not less than 3 years after the end of the financial year to which they relate.

- Wage and salary records: We are obliged to keep these records for 6 years.

How do we access and secure your personal data?

The Trust will use your information to administrate your employment and associated functions, personal data will be shared between relevant colleagues who legitimately need the information to carry out their duties e.g. your line manager and HR teams.

The Trust maintains electronic and paper records relating to your recruitment and employment, with information held by the HR team and locally with your line manager.

All paper files are kept in secure locked cabinets/cupboards and only relevant staff will have access to this information. Electronic information is accessed on a need to know basis only using the Trust's ESR system. Some Information may be held on the Trust's secure electronic drives, where access is only granted to appropriate individuals.

Should we be required to transfer any of your personal data outside the EEA, for example where we are communicating with you abroad in relation to your pre-employment documentation, you can expect a similar degree of protection in respect of the transfer of your personal information.

Your rights in relation to your personal data

1. The right to be forgotten

You have the right to request that your personal data is deleted if:

- it is no longer necessary for us to store that data having regard to the purposes for which it was originally collected; or
- in circumstances where we rely solely on your consent to process the data (and have no other legal basis for processing the data), you withdraw your consent to the data being processed; or
- you object to the processing of the data for good reasons which are not overridden by another compelling reason for us to retain the data; or
- the data was unlawfully processed; or
- the data needs to be deleted to comply with a legal obligation.

However, we can refuse to comply with a request to delete your personal data where we process that data:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation or the performance of a public interest task or exercise of official authority;
- for public health purposes in the public interest;
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes; or the exercise or defence of legal claims.

1. The right to data portability

You have the right to receive the personal data which you have provided to us, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided (us) where:

- the processing is based on consent or on a contract; and
- the processing is carried out by automated means.

Note that this right only applies if the processing is carried out by "automated means" which means it will not apply to most paper based data.

2. The right to withdraw consent

Where we process your personal data in reliance on your consent to that processing, you have the right to withdraw that consent at any time. You may do this in writing to the HR team or to your line manager.

3. The right to object to processing

Where we process your personal data for the performance of a legal task or in view of our legitimate interests you have the right to object on "grounds relating to your particular situation". If you wish to object to the processing of your personal data you should do so in writing to HR or to your line manager stating the reasons for your objection. Where you exercise your right to object we must stop processing the personal data unless:

- we can demonstrate compelling legitimate grounds for the processing, which override your interests, rights and freedoms; or
- the processing is for the establishment, exercise or defense of legal claims.

4. The right of subject access

So that you are aware of the personal data we hold on you, you have the right to request access to that data. This is sometimes referred to as making a "subject access request".

5. The right to rectification

If any of the personal data we hold on you is inaccurate or incomplete, you have the right to have any errors rectified.

Where we do not take action in response to a request for rectification you have the right to complain about that to the Information Commissioner's Office.

6. The right to restrict processing

In certain prescribed circumstances, such as where you have contested the accuracy of the personal data we hold on you, you have the right to block or suppress the further processing of your personal data.

7. Rights related to automated decision making and profiling

The GDPR defines "profiling" as any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict:

- performance at work;
- economic situation;
- health;
- personal preferences;
- reliability;
- behavior;
- location; or
- movement

You have the right not to be subject to a decision when it is based on automated processing; and it produces a legal effect or a similarly significant effect on you.

However, that right does not apply where the decision is necessary for purposes of the performance of a contract between you and us. We may use data related to your performance or attendance record to make a decision as to whether to take disciplinary action. We consider that to be necessary for the purposes of conducting the employment contract. In any event that is unlikely to be an automated decision in that action will not normally be taken without an appropriate manager discussing the matter with you first and then deciding whether the data reveals information such that formal action needs to be taken. In other words there will be "human intervention" for the purposes of the GDPR and you will have the chance to express your point of view, have the decision explained to you and an opportunity to challenge it.

Complaints

Where you take the view that your personal data are processed in a way that does not comply with the GDPR, you have a specific right to lodge a complaint with the relevant supervisory authority. The supervisory authority will then inform you of the progress and outcome of your complaint. The supervisory authority in the UK is the:

Information Commissioner,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire
SK9 5AF
Tel: 0303 123 1113, Fax: 01625 524510
www.ico.gov.uk