Privacy Notice: Your personal data and how we use it

1. About us

Maidstone and Tunbridge Wells NHS Trust is a large acute hospital Trust in the south east of England. We are an NHS provider organisation that provides a full range of general hospital services and some areas of specialist complex care to around 560,000 people living in the south of West Kent and the north of East Sussex.

Our core catchment areas are Maidstone and Tunbridge Wells and their surrounding boroughs, and we operate from three main clinical sites: Maidstone Hospital, Tunbridge Wells Hospital and Crowborough Birth Centre. We employ over 5000 staff. We also provide specialist cancer services to around 1.8 million people across Kent, Hastings and Rother, via the Kent Oncology Centre, which is sited at Maidstone Hospital and at Kent and Canterbury Hospital in Canterbury. We also provide outpatient clinics in a range of locations in Kent and East Sussex.

Our Headquarters are located at Maidstone Hospital, Hermitage Lane, Maidstone Kent ME16 9QQ, and our main telephone number is 01622 729000.

We are registered as a Data Controller on the Data protection register of the Information Commissioner's Office (our registration number is Z9042352).

2. Your personal data

During the course of our employment activities, we collect, store and processes information about job applicants, current employees, former employees, temporary workers (including Agency and Bank staff), volunteers, trainees and those carrying out work experience. This information is called "personal data" because it relates to you as an individual who can be identified. The ways in which we use your personal data are governed by law. The principal legislation that applies is the European Union's General Data Protection Regulation (GDPR) and the UK's Data Protection Act 2018 (DPA). In addition, confidential information that you give in relation to our employment activities is governed by the common law duty of confidentiality[1].

When we use your information, the law calls this "processing". The personal data we process to carry out our activities and obligations as an employer includes:

- Your name, date of birth, gender, home address and national insurance number
- Contact details such as telephone numbers, emergency contact(s) and personal email address (if you have told us this)
- Proof of eligibility to work in the UK
- Checks from the Disclosure and Barring Service (DBS)
- Professional registration and qualifications
- Details of your skills, education and training
- Bank details
- Pension details
- Occupational Health information on your physical health or mental health ((including whether you have any allergies, a disability or require any additional support or adjustments for your employment)[2]
- Absence history
- Information relating to employee relations (disciplinary proceedings, grievances and complaints, Employment Tribunal claims etc.)

[1] A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. This is a legal obligation derived from case law (i.e. rather than being an explicit requirement of any particular legal Act), and the obligation for information to remain confidential remains in place after a person has died.

[2] The Occupational Heakth department has produced its own Privacy Notice, which is available to staff on the Trust Intranet, at http://10.136.105.189/uploads/resources/Occupational_Health_Privacy_Notice.pdf

- Information relating to your health and safety at work, and details of any incidents or accidents
- Details of your working patterns (days of work and working hours) and attendance at work
- Details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave
- Assessments of your performance, including appraisals, performance reviews and ratings, and related correspondence
- Visual images (for your ID badge)
- Details of your vehicle/s (if you pay for parking at the Trust), such as registration number, make, model etc.
- Information relating to you claiming work-related expenses such as details of your driving licence and vehicle/s (insurance, tax, MOT etc.), debit/credit card receipts etc.
- Declarations of interest and/or gifts and/or hospitality
- Correspondence with you (including emails)
- Depending on the position you hold with us, we may also collect information in relation to any current or previous criminal offences
- "Special category personal data", such as your race, ethnic origin, sex life and/or sexual orientation, Trade union membership, and religion or beliefs (see section 6 for further information)

3. How we obtain and use your personal data

The personal data we hold about you will either be provided directly by yourself (e.g. when applying for a job or completing various documentation during your employment with us), by external organisations (such as previous employers, your professional body or the DBS) or by other parties (such as your GP or character referees you have provided).

We need accurate, up-to-date data about you because this enables us to:

- Run recruitment and promotion processes
- Undertake staff administration and management
- Operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace
- Operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes
- Provide payroll services (and ensure you receive the correct pay)
- Administer your pension (if applicable)
- Undertake planning
- Carry out accounting and Auditing
- Prevent crime and assist in the prosecution of offenders
- Provide you with relevant education and training opportunities
- Provide Occupational Health services
- Undertake surveys to assess what staff think about working for us
- Provide references on request for current or former employees
- Respond to and defend against legal claims
- Provide details of available bank shifts
- Maintain and promote equality in the workplace
- Respond to and rectify problems that you identify with our IT systems
- Respond to and rectify problems that you identify in relation to Estates and Facilities
- Share and match personal data as part of the National Fraud Initiative[3]

Our use of your personal data is governed by the law and we have a duty to ensure your personal data is kept safe and secure. Your personal data may be stored within electronic and/or paper records. Such records are restricted so that only those individuals who have a need to access your personal data can do so.

[3] 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

One of the main electronic records we use is the Electronic Staff Record (ESR). This supports the delivery of national workforce policy and strategy and provides NHS organisations with a range of tools that facilitate effective workforce management and planning.

3.1 Sharing your personal data

To support you in your employment and to enable us to meet our legal responsibilities as an employer, we will sometimes need to share your information with others. Any disclosures of personal data are always made on case-by-case basis, using the minimum personal data necessary for the specific purpose and circumstances and with the appropriate security controls in place.

To enable effective administration, we may share your information with the following external parties to process your data on our behalf:

3.1.1 NHS Shared Business Services

The personal data you provide during the course of your employment (including the recruitment process) will be shared with NHS Shared Business Services who provide our payroll and pensions services.

3.1.2 NHS Jobs

NHS Jobs has an interface to the ESR. The data you submit to NHS Jobs may be transferred to ESR to establish the human resources and payroll record; completing the recruitment process (or parts of the process) on ESR; or for reporting purposes such as equal opportunity monitoring. NHS Jobs produce their own Privacy Notice, which is available at www.jobs.nhs.uk/privacy.html.

3.1.3 Selenity

This company provides the software that we use to process the work-related expenses claimed under our Expenses Policy and Procedure.

3.1.4 Allocate Software plc.

This company operates our “EmployeeOnline” system which enables staff to view all aspects of their roster (i.e. working pattern).

3.1.5 Government agencies and or the Police

We are sometimes required by law to disclose or report certain information, which may include your personal data. For example, we send statutory information to organisations such as HM Revenue and Customs (HMRC) or Pensions Agencies. We may also need to release your personal data to the Police or counter fraud agencies. Where mandatory disclosure is necessary only the minimum amount of information is released.

3.2 Direct marketing

We do not collect or sell your personal data for direct marketing purposes.

4. Transfers of personal data to data controllers and processors located outside the European Economic Area (i.e. third countries) or international organisations

We may need to transfer your personal data to data controllers and processors located outside the European Economic Area (i.e. third countries)[4] or international organisations.

[4] See www.gov.uk/eu-eea for a list of countries within the EEA

5. The legal basis for processing your personal data and your associated rights

The GDPR includes 8 separate rights for individuals. However, the GDPR also obliges us to decide the specific legal basis under which we will process your personal data, and the rights you have are directly linked to the legal basis we rely on. Not all of the 8 rights apply to all legal bases.

5.1 Public task

We primarily process your personal data on the basis of Article 6(1)e of the GDPR, which relates to that processing being necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Trust. The UK's Information Commissioner's Office (ICO) calls this legal basis "Public task", and the ICO expects most NHS provider organisations to rely on this legal basis for most of the data processing they do. This is because our underlying tasks, functions and powers have a clear basis in law (under numerous Acts of Parliament such as the Health and Social Care Act 2012). When we rely on the "Public task" legal basis, only 6 of the 8 rights under the GDPR apply:

- **The right to be informed.** This means that we must provide you with information about why we process your personal data, how long we hold that data, and who we share that data with. The ICO calls this "privacy information", and the Trust meets its obligations under this right through this Privacy Notice, which has been developed to comply with the ICO's expectations

- **The right of access.** You have the right to access the personal data that we hold about you. This is commonly referred to as "subject access", and asking to see your personal data is called a "Subject Access Request". The GDPR obliges us to respond to such requests within 1 month, and in most circumstances, we cannot charge a fee to deal with such requests. Requests to access your personal data should in the first instance be made to your line manager (if applicable), who should be able to obtain that information from the Human Resources Department or put you in contact with the relevant person within that Department. If you do not have a line manager, or if you are dissatisfied with the outcome, the Trust's Head of Employee Relations should be contacted.

- **The right to rectification.** You have the right to have inaccurate personal data rectified, or completed if it is incomplete. The DPA states that personal data is "inaccurate" if it is incorrect or misleading as to any matter of fact. If, for example, you therefore ask us to rectify a recorded opinion from a member of staff, we may not conclude that the record of that opinion is inaccurate and needs to be rectified, as opinions are, by their very nature, subjective. The GDPR obliges us to respond to such requests within 1 month. However, we can refuse a request for rectification if the request is manifestly unfounded or excessive (including taking into account whether the request is repetitive). There may also be some other exemptions under the GDPR or DPA that we judge should apply, but these exemptions will only be applied on a case by case basis. If you wish to request that your personal data be rectified, you should, in the first instance, discuss your request with your line manager (if applicable), and specify what data you believe should be rectified and why. Your line manager should be able to liaise with from the Human Resources Department or put you in contact with the relevant person within that Department. If you do not however have a line manager, or are not satisfied with the response, you should contact the Trust's Data Protection Officer (see section 7 for their contact details), and specify what data you believe should be rectified and why.

- **The right to restrict processing.** Restricting data processing means that we can store your personal data but not use it. You have the right to request that we restrict or suppress your personal data if:

- You believe your personal data is inaccurate and you wish to verify the accuracy of that data;
- You believe your personal data has been unlawfully processed (i.e. that we have breached the first principle of the GDPR[5])
- We no longer need your personal data but you need us to keep it in order to establish, exercise or defend a legal claim; or
- You have objected to us processing you data under Article 21(1) of the GDPR (the right to object – see below), and we are considering whether our legitimate grounds override your legitimate grounds

The GDPR obliges us to respond to requests to restrict processing within 1 month. If you wish to request that your personal data be restricted, you should contact the Trust's Data Protection Officer (see section 7 for their contact details) and specify what data you believe should be restricted and why (making reference to one of the 4 reasons listed above).

- **The right to object.** When the Trust relies on the "Public task" legal basis, you have the right to ask us to stop processing your personal data. However, you must give specific reasons why you are objecting to us processing your data, and these reasons should be based upon your particular situation. You should also note that this is not an absolute right, and we can continue processing if we can demonstrate compelling legitimate grounds for the processing, which override your interests, rights and freedoms. If you wish to object to us processing your personal data, you should contact the Trust's Data Protection Officer (see section 7 for their contact details), and specify what data processing you are objecting to and why. However, if we are satisfied that we do not need to stop processing your personal data, we will let you know, and explain our decision. In such circumstances, you have the right to make a complaint to the ICO (see section 9 for their contact details) and/or seek to enforce your right through a judicial remedy (i.e. through the law courts).

- **Rights in relation to automated decision making and profiling.** Automated individual decision-making is when a decision is made solely by automated means without any human involvement. Profiling is the automated processing of personal data to evaluate certain things about an individual. Profiling can be part of an automated decision-making process. The GDPR has additional rules to protect individuals if they are subject to automated decision making and profiling. However, we do not process your personal data in this way, so those rules, and the associated rights, do not apply.

  You do not therefore have:
  - The right to erasure i.e. you do not have the right to have the personal data we hold about you erased. You do however have a right to restrict how we process that data (see above);

    or

  - The right to data portability i.e. you do not have the right to obtain and reuse the personal data we hold about you for your own purposes across different services, nor to ask that we copy or transfer the personal data we hold in our IT environment to another such environment in a safe and secure way, without affecting its usability.

5.2 Contract

When we process your personal data to fulfil the terms of your employment contract, we do this on the basis of Article 6(1)b of the GDPR, which relates to that processing being 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. When we rely

[5] That personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject

on the “Contract” basis to process your personal data, you do not have the right to object, but you do have the right to erasure and the right to portability. If you wish to exercise these rights, you should contact the Trust’s Data Protection Officer (see section 7 for their contact details) and describe the personal data concerned and the action you would like us to take.

5.3 Legal obligation

There may be occasions when we need to process your personal data to comply with a common law or statutory obligation. When this is required, we do this on the basis of Article 6(1)c of the GDPR, which relates to such processing being necessary for compliance with a legal obligation to which the controller is subject. When we rely on the “Legal obligation” basis to process your personal data, you do not have the right to object, the right to erasure, or the right to portability.

5.4 Consent

When we process your personal data for any other means, we do this on the basis of Article 6(1)a of the GDPR, which relates to you giving consent to the processing of your personal data for one or more specific purposes. If this is the case, you will be asked to give explicit consent i.e. we will not presume consent from silence, inaction or pre-selected choices. Under such circumstances, you also have the right to withdraw your consent for that processing.

6. The legal bases for processing special categories of personal data

Special category data is personal data which is more sensitive, and so needs more protection (as this type of data could create more significant risks to a person’s fundamental rights and freedoms, by putting them at risk of unlawful discrimination). Such data includes information about an individual’s race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation. The GDPR obliges organisations that process special category data to decide the additional, specific, legal basis under which we will do this.

As was noted above, we process special category, and we do this on the basis of:

- Condition b of Article 9(2) of the GDPR, which relates to such processing being 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 and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; and
- Condition h of Article 9(2) of the GDPR, which relates to such processing being necessary for the provision of health or social care or treatment or the management of health or social care systems and services on the basis of European Union or UK law; and .

7. Our Data Protection Officer (DPO)

As we are a public authority, the GDPR requires us to appoint a Data Protection Officer (DPO), and our Trust Secretary has been appointed to that role. Our DPO assists us to monitor internal compliance with the GDPR, informs and advise us on our data protection obligations, provides advice regarding Data Protection Impact Assessments and acts as a contact point for data subjects and the ICO.

Our Data Protection Officer can be contacted via email (kevinrowan@nhs.net) or telephone (01622 228 698).

8. Retention periods

We hold your personal data for specified periods of time, as set out in the Records Management Code of Practice for Health and Social Care 2016.

9. Your right to complain

If you wish to complain about how we have processed for personal data, you should, in the first instance, contact your line manager (if applicable), describe the nature of your complaint, and (ideally) state what action you would like the Trust to take. Your line manager should be able to either discuss your concerns with the Human Resources Department or put you in contact with the relevant person within that Department.

If you do not have a line manager, or if you are dissatisfied with the outcome, contact our Head of Information Governance (Gail Spinks), on 01892 634 029, describe the nature of your complaint, and (ideally) state what action you would like the Trust to take.

If you remain dissatisfied with the outcome, you have the right to ask the Information Commissioner's Office (ICO) to investigate your complaint, using the ICO's website, at https://ico.org.uk/make-a-complaint/your-personal-information-concerns/.