Kent Community Health
NHS Foundation Trust

Privacy/fair processing notice

Kent Community Health NHS Foundation Trust of Trinity House, 110-120 Upper Pemberton, Eureka Business Park, Kennington Road, Ashford, Kent, TN25 4AZ www.kentcht.nhs.uk is a "data controller" for the purposes of data protection legislation. A data controller determines the purposes and means of processing personal data.

Personal data is any information which relates to an individual who can be identified from that information.

Processing includes the collection, recording, storage, use, disclosure or destruction of personal data.

Under the General Data Protection Regulation (GDPR) we are required to provide all data subjects with a privacy notice to inform the subject about how and why we process personal data and the lawful basis for doing so.

This privacy notice applies to current and former employees, workers, contractors, agency staff, jobseekers and volunteers (together 'the workforce') and it is important that you read through it carefully. This notice does not form part of any contract of employment or other contract to provide services and may be amended from time to time.

Kent Community Health NHS Foundation Trust has a Data Protection Officer (DPO) whose role it is to ensure that data protection is built into the organisation's culture and working practices. If you have any questions about the use of your personal data, you should contact the DPO in the first instance.

The contact details of the DPO are: kentchft.dataprotectionofficer@nhs.net

Data protection principles

The GDPR came into force on 25 May 2018 and sets out the principles which we, as a data controller, must adhere to when processing your personal data.

The GDPR principles are as follows:

Lawfulness, fairness and transparency – data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

Purpose limitation – data must be collected only for specified, explicit and legitimate purposes.

Data minimisation – data must be adequate, relevant and limited to what is necessary.

Accuracy – data must be accurate and, where necessary, kept up to date. Inaccurate data must be erased.

Storage limitation – data must only be stored for as long as is necessary.

Integrity and confidentiality – data must be processed in a secure manner.

Accountability - the data controller is responsible for, and must be able to demonstrate, compliance with the other data protection principles.

The workforce personal data processed by Kent Community Health NHS Foundation Trust

The provision of personal data is necessary in order that the organisation can enter a contract with you to provide services for the organisation. If you fail to provide the details requested, we may be unable to comply with the terms of any contract with you or comply with our legal obligations to you.

We process the following categories of personal data about you:

- Name, address, contact details, date of birth
    - In order to enter into your contract of employment you are required to provide your personal details. If you do not provide this information, we will not be able to employ you.
- Terms and conditions of employment
- Qualifications and work experience as set out in job applications and CVs
- Bank account details and national insurance number
    - In order to enter into your contract of employment you are required to provide bank details and your national insurance number to the organisation. If you do not provide this information, we will not be able to process payments to you and account for tax and national insurance deductions to HMRC which we are required to do by law.
- Pensions scheme membership details
    - You are required under the terms of your contract to provide information about your pension scheme membership. If you do not provide this information, we will not be able to administer your pension benefits.
- Information about your right to work in the UK
    - In order to enter into your contract of employment, you are legally required to provide evidence of your right to work in the UK. If you do not provide this information, we will not be able to employ you.
- Information about criminal offences
    - In order to enter into your contract of employment, you may be required to provide information and agree to undertake a DBS check to enable us to confirm that you have no relevant unspent convictions or other factors that may put patients at risk and to verify your suitability for the position. If you do not provide this information, we will not be able to employ you.
- Periods of leave which are requested and which have been taken (annual leave and sickness absence, maternity, paternity, parental leave)
    - You are required under the terms of your contract and you are obliged under statute to provide information about periods of leave. We require this information to provide you with your statutory and contractual benefits. If you do not provide this information, we may not be able to provide these benefits.
- Disciplinary and grievance procedures including warnings
- Records of appraisals and performance improvement plans
- Special category 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 and data about immunisations and vaccinations
- Use of our IT, communication and other systems

- Details of your use of business-related social media, such as LinkedIn, general social media and any non-business related internet browsing or downloads during work time
- Details in references about you that we give to others

We collect personal information about our workforce during the recruitment process, and periodically at other times during employment, either directly from candidates or ESR or sometimes from an employment recruitment agency or background check provider. Personal data about our workforce is collected in many ways: through communications with you either face to face or in writing, email or on the telephone; through monitoring of our websites and our computer networks and connections, CCTV and access control systems, communications systems, remote access systems, from your doctors, from medical and occupational health professionals we engage, email and instant messaging systems, intranet and internet facilities.

We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies.

We aim to ensure that our data collection and processing is always proportionate. We will notify you of any material changes to information we collect.

Why we process personal data

We process the personal data of our workforce for employment purposes but also to assist in running the National Health Service, for example by improving the management of our workforce we can improve the experience of both staff and service users.

We will only use your personal data when the law allows us to and processing is necessary. The GDPR sets out six legal bases for processing personal data.

Lawful basis for processing your personal data

Depending on the processing activity, we rely on the following lawful basis for processing your personal data under the GDPR:

1. Article 6(1)(b) which relates to processing necessary for the performance of a contract. For example employment contracts, contracts with doctors and dentists, contracts with contractors and agencies through which locums are engaged.
2. Article 6(1)(c) so we can comply with our legal obligations as your employer.
3. Article 6(1)(d) in order to protect your vital interests or those of another person.
4. Article 6(1)(e) where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Kent Community Health NHS Foundation Trust.
5. Article 6(1)(f) Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We set out below the ways in which we process your personal data and the legal basis upon which we rely as set out above.

- Making a decision about your recruitment or appointment [Legitimate interest – the legitimate interest being the employment of a suitable workforce].
- Determining the terms on which you work for us [Legitimate interest – the legitimate interest being making appointments, maintaining good employment practices and ensuring consistency of terms of employment across the workforce]
- Checking that you are legally entitled to work in the UK [Legal obligation]
- Where eligible, checking your criminal record [Legal obligation]

- Uploading information onto Employment Staff Record (ESR) [Legitimate interest - the legitimate interest being the employment of a suitable workforce; Contract – to administer payroll and pension] ESR is operated by IBM on behalf of the Department of Health and is used by NHS organisations as set out above.
- Transferring data via the ESR streamlining programme where your employment transfers from one NHS organisation to another [Contract – see below. Legal obligation – for example where TUPE applies. Legitimate interest – effecting transfer efficiently]
- Paying you and deducting tax and National Insurance contributions [Contract/Legal obligation]
- Liaising with your pension provider [Contract]
- Administering the contract we have entered into with you [Contract/Legal obligation]
- Business management and planning, including appraisal, accounting and auditing [Legitimate interest - the legitimate interest being the effective and efficient management of the workforce and provision of health care services]
- Conducting performance reviews, managing performance and determining performance requirements [Contract/Legal obligation/Legitimate interest – contracts require compliance with Trust policies, the legitimate interests being maintaining employment records and complying with legal and regulatory obligations; good employment practice and to ensure safe working practices in the provision of the healthcare service conducting disciplinary procedures - [Legal obligation/Contract/Legitimate Interest - contracts require compliance with Trust policies and disciplinary process. The legitimate interests being maintaining employment records and complying with legal and regulatory obligations; good employment practice and to ensure safe working practices in the provision of the healthcare service/Performing a task in the public interest]
- Making decisions about salary reviews [Contract]
- Assessing qualifications for a particular job or task [Legitimate interest - the legitimate interest being employment of a suitable workforce/Performing a task in the public interest].
- Gathering evidence for possible grievance or disciplinary hearings [Legal obligation/Contract/Legitimate interest - contracts require compliance with Trust policies and disciplinary process. The legitimate interests being maintaining employment records and complying with legal and regulatory obligations; good employment practice and to ensure safe working practices and the effective provision of health care services/Performing a task in the public interest].
- Making decisions about your continued employment or engagement [Legal obligation/Contract/Legitimate interest - contracts require compliance with Trust policies and disciplinary process. The legitimate interests being maintaining employment records and complying with legal and regulatory obligations; good employment practice and to ensure safe working practices and the effective provision of health care service/Performing a task in the public interest].
- Making arrangements for the termination of our working relationship [Legal obligation/Contract/Legitimate interest - contracts require compliance with Trust policies and disciplinary process. The legitimate interests being maintaining employment records and complying with legal and regulatory obligations; good employment practice and to ensure safe working practices and the effective provision of health care services/Performing a task in the public interest].

- Assessing and delivering upon education, training and development requirements [Legitimate interest - the legitimate interest being the employment and development of a suitable workforce.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work [Legal obligation].
- Ascertaining your fitness to work [Legal obligation].
- Managing sickness absence and assessing your right to occupational sick pay [Contract/Legal obligation].
- Complying with health and safety obligations [Legal obligation]
- To prevent fraud [Legal obligation].
- To monitor use of our information and communication systems to ensure compliance with our IT policies [Legitimate interest – the legitimate interest being to monitor use of equipment, systems and facilities provided to you for business purposes in accordance with our policies and to safeguard the personal data of employees and service users.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution. [Legitimate interest – the legitimate interest being to protect our networks and safeguard the personal data of employees and service users. Equal opportunities monitoring [Legal obligation].

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal data.

We will keep the personal data we store about you accurate and up to date. Data that is inaccurate or out of date will be destroyed. You are responsible for notifying us if your personal details change or if you become aware of any inaccuracies in the personal data we hold about you.

Consent

Under the Data Protection Act 1998, consent was the basis on which most employers processed the personal data of their workforce. Guidance issued in relation to the GDPR has stated that consent should only be relied on as the legal basis for processing where it is freely given, specific, informed and unambiguous. We will not, generally, rely on consent as a legal basis for processing your personal data but in certain circumstances it may be deemed appropriate. Where you provide consent to the processing of your data, you will be asked at the time the data is processed and you should be aware that you will be able to withdraw your consent at any time.

Special category data

We will only process special category data about genetic and biometric data, and data regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, and sexual orientation, where a further condition is also met.

Where the information we process is special category data, for example your health data, the additional bases for processing that we rely on are:

- Article 9(2)(b) which relates to carrying out our obligations and exercising our rights in employment and the safeguarding of your fundamental rights.
- Article 9(2)(c) to protect your vital interests or those of another person where you are incapable of giving your consent.

- Article 9(2)(h) for the purposes of preventative or occupational medicine and assessing your working capacity as an employee.
- Article 9(2)(f) for the establishment, exercise or defence of legal claims.
- Article 9(2)(j) for archiving purposes in the public interest.

In addition, we rely on processing conditions at Schedule 1 part 1 paragraph 1 and Schedule 1 part 1 paragraph 2(2)(a) and (b) of the DPA 2018. These relate to the processing of special category data for employment purposes and preventative or occupational medicine and the assessment of your working capacity as an employee.

The conditions which will usually apply are that we have a legal obligation to process the information, where it is necessary to assess your working capacity on health grounds or, less commonly, where it is needed in relation to legal claims.

We will use your special category data in the following ways:

- information relating to leaves of absence, which may include sickness absence or family related leave, to comply with employment and other laws.
- information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
- information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.

Criminal convictions and offences

- We process information about staff criminal convictions and offences. The lawful basis we rely to process this data are:
- Article 6(1)(e) for the performance of our public task. In addition, we rely on the processing condition at Schedule 1 part 2 paragraph 6(2)(a).
- Article 6(1)(b) for the performance of a contract. In addition we rely on the processing condition at Schedule 1 part 1 paragraph 1.

The CQC requires that we, as CQC-regulated service providers, carry out DBS checks where we are authorised to do so under legislation. You should be aware that certain roles within the organisation will require either a standard, enhanced or enhanced with barred list information DBS check to be carried out. For those providing healthcare services, standard checks may be obtained for individuals working in a role listed in schedule 1 to the ROA (Exceptions) Order 1975 (“ROA Exceptions Order”). Paragraph 15 states:

“Any employment or other work which is concerned with the provision of health services and which is of such a kind as to enable the holder of that employment or the person engaged in that work to have access to persons in receipt of such services in the course of his normal duties”.

An enhanced check may be obtained for the roles listed in the ROA Exceptions Order and also in the Police Act 1997 (Criminal Records) Regulations.

Enhanced DBS checks with barred list information can be obtained for individuals where roles fall under the definitions of regulated activity within the meaning of the Safeguarding Vulnerable Groups Act 2006 as amended by the Protection of Freedoms Act 2012.

We will only require a DBS check to be made where the role is eligible and the check shall be at the appropriate level only and no higher. We will assess the relevance of any cautions and convictions detailed in the DBS check to the role for which the applicant has applied.

Given the sensitive nature of the information contained in a DBS certificate, the organisation will ordinarily only retain on file information about the level of check which was requested and the date on which the certificate was obtained.

For a very small number of staff who work in Immigration Removal Centres we will carry out additional counter terrorist checks.

Electronic Staff Record

On commencement of employment with the Trust, your personal data will be uploaded to the Electronic Staff Record (ESR). ESR is a workforce solution for the NHS which is used to effectively manage the workforce leading to improved efficiency and improved patient safety.

ESR will be updated where gaps in personal data are identified and there is a legitimate interest that the Trust do so or where you have notified the Trust of a change in your personal data e.g. a change of address, change of marital status or change to your health.

Streamlining

In accepting employment, you accept that the following personal data will be transferred under the streamlining programme if your employment transfers to another NHS organisation:

Name, contact details, date of birth, NI number, gender, nationality and marital status, professional registration details, sickness record, leave record, qualifications, employment history, employment dates, pay and pension information.

Streamlining is the process by which certain personal data is transferred from one NHS organisation to another when your employment transfers. NHS organisations have a legitimate interest in processing your data in this way in establishing the employment of a suitable workforce. The streamlining programme is a data sharing arrangement which is aimed at improving efficiencies within the NHS both to make costs savings for Trusts but also to save you time when your employment transfers. [This processing is lawful under the Contract]

Retention periods

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Retention periods for personal data will vary according to the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements. We ordinarily follow the retention periods set out in the NHS Records Management Code of Practice.

You should be aware that employee documentation is ordinarily retained for six years after termination of employment, which is the statutory limitation period for breach of contract claims, and then promptly deleted once that period has passed. A summary of your records will be kept until your 75th birthday or six years after leaving whichever is the longer and then reviewed. For unsuccessful job candidates, documentation is retained for six months after he or she is rejected for a role and then deleted.

However, it should be noted that there is some legislation which requires certain health monitoring data to be retained for up to 40 years and for clinical staff where there is a negligence claim in relation to a child, the normal three year personal injury limitation period is extended until that child reaches 21 years of age. We have put a system in place so that the data of staff which may be at risk of certain diseases or where they were involved in an incident that could give rise to a clinical negligence claim which require a longer retention period than six years are marked appropriately as needing to be retained for a longer period.

If we are able to anonymise your personal data so that you can no longer be identified from it, we may use such information without further notice to you.

Recipients of data

We may have to share your data with third parties, including third-party service providers and other entities in the NHS for example with ESR as part of the NHS streamlining programme and the NHS Pension Scheme. We may also need to share your data with third parties such as external contractors and our professional advisers.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities within the NHS. The following third-parties may receive personal information about you for the following purposes:

Recipient	Data disclosed	Purpose of disclosure
Civica UK Limited (Trac)	Name and contact details, date of birth, previous experience, education, referees, equal opportunities, right to work status, ID documents and answers to questions relevant to the role you have applied for. Our recruitment team, managers and shortlisting and interview panels will have access to all of this information.	Recruitment, shortlisting and hiring process.
DocuSign	Name, employment offer details, address, contact details, date of birth, NI number, bank details, previous experience, professional registration details, equal opportunities monitoring information, right to work status, ID documents, next of kin details, criminal record	Recruitment and hiring process.

	information, COVID vaccination status, terms and conditions information including pay, pension and employment status information. Our recruitment team, have access to all of this information.	
TrustID	Name, date of birth, place of birth, passport number, photograph (self-potrait)	To determine your right to work in the UK
Optima Health	Information about your medical history and immunisation status	To determine fitness to work.
HR Connect (Payroll Provider)	Name, contact details, bank details, address, date of birth, National Insurance Number, next of kin, equal opportunities data, professional registration details, and salary.	Payroll and pension administration, specialist education recruitment via Kent, Occupational Health Services and DBS Services.
Electronic Staff Record, IBM	Name, contact details, bank details, address, date of birth, National Insurance Number, next of kin, equal opportunities data, professional registration details, sickness record, leave record, qualifications, employment history, employment dates, pay and pension information.	This system is used to administer payroll and used as our HR database.
Cornerstone	Name, contact details, appraisal and training data.	Training and appraisal record
HealthRoster, Allocate – an RLDatix company	Name, contact details, assignment number, NI Number job tile, grade, hours of work, sickness record and working patterns.	To manage annual leave records, rosters, payment of enhanced pay and temporary staffing management. .
Quality Health	Name, base, job, service, equal opportunities data, and maternity status.	To fulfil our obligation to participate in the NHS staff survey.
National Fraud Initiative (a data matching exercise conducted by the Cabinet Office under its data matching	Name, assignment number, department, title, gender, address, Unique Property Reference Number (UPRN),	Mandatory requirement. For the prevention and detection of fraud.

powers as set out in Part 6 of the Local Accountability and Audit Act 2014)	date of birth, telephone number(s), e-mail address, Passport Number, date started, date left and leave indicator, NI Number, full time/part time confirmation, gross pay to date, standard hours per week, date last paid, and bank details.	
EASY, Giltbyte	Name, Assignment Number, Job title, Work Base, Home address	Travel & Expenses Administration
Vismo	Name, Address, contact details, Job title & Role	Emergency Planning

All our third-party service providers and other entities in the NHS are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

Security

We will ensure that appropriate measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We have in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. We will only transfer personal data to a third party if the third-party agrees to comply with those procedures and policies, or if it puts in place adequate measures.

Maintaining data security means guaranteeing the confidentiality, integrity and availability (for authorised purposes) of the personal data.

Not all our third-party providers use forced encryption. Civica UK Limited uses encryption where the recipient's server supports it. Where this is not the case the information in any communication is sent in plain text.

Automated decision making

An automated decision is one that is made with no human involvement. For example your occupational health questionnaire will initially go through an automated process to determine your fitness to work. However, should the outcome be anything other than a positive one this will be reviewed by an Occupational Health practitioner before any further action and a final decision is reached.

Please be aware that you will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

Rights of access, correction, erasure, restriction and portability

You have the following rights under the GDPR:

- Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

- Request correction of the personal data that we hold about you. This enables you to ask to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it.
- Object to processing of your personal information on grounds relating to your particular situation where we are relying on a legitimate interest (or those of a third party) or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Kent Community Health NHS Foundation Trust as the lawful basis for processing
- Request the restriction of processing of your personal information on the following grounds:
    - you contest the accuracy of the personal data for a period enabling us to verify the accuracy;
    - the processing is unlawful and you oppose the erasure of the personal data and requests restriction instead;
    - we no longer need the personal data for the original purposes of the processing, but the data is required by you for the establishment, exercise or defence of legal claims;
- Request the transfer of your personal information to another party, also known as portability.

Please contact the DPO in writing (contact details above) if you would like to exercise any of your rights under the GDPR.

Please be aware that whilst a fee will not normally apply where there is a request to access your personal data, we may charge a reasonable fee if your request for access is repeated and/or clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

Right to contact the Information Commissioner's Office

You should be aware that you have the right to make a complaint to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues. The contact details of the ICO are as follows:

Helpline: 0303 123 1113

https://ico.org.uk/concerns/