Staff Privacy/Fair Processing Notice

Kettering General Hospital NHS Foundation Trust of Rothwell Road, Kettering, Northants NN16 8UZ and www.kgh.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 why we process personal data and the legal basis for doing so.

This privacy notice applies to current and former employees, workers, contractors 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.

Kettering General Hospital 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:

Head of Information Governance Assurance & DPO
Email: informationgovernanace@kgh.nhs.uk
Tel: 01536 491560

Data protection principles

The GDPR came into force on 25 May 2018 and sets out the principles 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 Kettering General 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 following categories of personal data about you:

- Name, address, contact details

  - 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.
- 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 a DBS check to enable us 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 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 and general social media
- Details in references about you that we give to others

We collect personal information about our workforce through the recruitment process, 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 improve the experience of service users.

We will only use your personal data when the law allows us to. The GDPR sets out six legal bases for processing personal data. The most common legal bases for processing your personal data are:

1. Where we need to perform the employment **contract** we have entered into with you.

2. Where we need to comply with a **legal obligation**.

3. 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.

4. Where it is necessary for us to perform a **task in the public interest** or for our official functions, and the task or function has a clear basis in law

We set out below the ways in which we process your personal data and the legal basis on which rely as set out in 1 – 4 above.

- Making a decision about your recruitment or appointment [Legitimate interest – the legitimate interest being the employment of a suitable workforce/Performing a task in the public interest].
- Determining the terms on which you work for us [Legitimate interest – the legitimate interest being maintaining good employment practices and ensuring consistency of terms of employment of the workforce/Performing a task in the public interest]
- Checking 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 [Legitimate interest - the legitimate interest being the employment of a suitable workforce/Performing a task in the public interest]
- Transferring data via the streamlining programme where your employment transfer from one NHS organisation to another
- 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 accounting and auditing [Legitimate interest - the legitimate interest being the effective and efficient provision of health care services/Performing a task in the public interest]
- Conducting performance reviews, managing performance and determining performance requirements [Legitimate interest - 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]

- Conducting disciplinary procedures - [Legitimate Interest - 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 and compensation [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 [Legitimate interest - 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 [Legitimate interest - 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 [Legitimate interest - 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].
- Education, training and development requirements [Legitimate interest - the legitimate interest being the employment of a suitable workforce/Performing a task in the public interest].
- 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 your use of our information and communication systems to ensure compliance with our IT policies [Legitimate interest – the legitimate interests being to monitor and manage staff access to our systems and facilities; to protect our networks, and the personal data of employees and service users, against unauthorised access or data leakage; to ensure our policies, such as those concerning security and internet use, are adhered to for operational reasons, such as maintaining employment records, maintaining service user records, training and quality control to ensure that sensitive information is kept confidential.]
- 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 interests being to monitor and manage staff access to our systems and facilities; to protect our networks, and the personal data of employees and service users, against unauthorised access or data leakage; to ensure our policies, such as those concerning security and internet use, are adhered to for operational reasons, such as maintaining employment records, maintaining service user records, training and quality control to ensure that sensitive information is kept confidential.]

- 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.

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 leaves, 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 offence and Fit and Proper Person data

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.

In addition to criminal records the CQC Fit and Proper Persons requirement also requires that we hold data relating to all executive and non executive director (and their deputies who report directly into board) this includes a declaration of interests, any disqualification from charity and; or directorship, any declaration of bankruptcy. This is order to legitimately determine there are no conflicts of interest in the terms on which you work for Kettering General Hospital NHS Foundation Trust that would be in the public interest.

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.

Once you have commenced employment your information is available to see via logging on via user name and password to https://my.esr.nhs.uk if you require support please email esremployeeselfservice@kgh.nhs.uk for further support regarding access to your record.

Factual references

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

- Name
- Date of Birth
- Dates of employment
- Most recent role title held on ESR
- days and episodes of sickness in the last two years
- Any formal warnings or formal investigations pending including safeguarding concerns,
- Date, Level and outcome of DBS check undertaken

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:

- Factual reference (as described above)
- Level of occupational health clearance
- Statutory and Mandatory training achieved

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.

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
Bank Partners	Data held on ESR	Provider of Staff Bank Services to Kettering General Hospital NHS Foundation Trust
University Hospital of Birmingham	Data held on ESR	Provider of Payroll to Kettering General Hospital NHS Foundation Trust
NHS Business Services Authority	Data held on ESR	Provider of Pensions to Kettering General Hospital NHS Foundation Trust
Quality Health	Data held on ESR	Provider of pseudonymised National NHS Staff Survey to Kettering General Hospital NHS Foundation Trust

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.

Freedom of Information Requests (FOI)

Staff personal information may be disclosed, if this is required, as part of FOI requests. This is where it can be demonstrated there is evidence to satisfy Condition 6 of Schedule 2 of the Data Protection Act 2018 and that the Trust's Data Protection Officer has approved this release.

This disclosure would only apply when:

- The information relates to employees in their professional role
- Given the need for accountability and transparency about public authorities, there is expectation of disclosure, so the disclosure could be considered fair to the employee
- Sharing would not unjustly result in adverse effects on the employees
- The employees work in a senior role where it is reasonable to expect that a public authority would disclose this information
- There is a legitimate public interest in knowing how public money is apportioned across an organisation

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.

Automated decision making

An automated decision is one that is made with no human involvement. For example, where an organisation monitors sickness absence via a computer programme, and the disciplinary process is automatically triggered when an employee reaches a certain number of days' absence.

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 where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground.
- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- 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/

I,<<name>> (employee/worker/contractor/volunteer name), acknowledge that on I received a copy of Kettering General Hospital's Privacy Notice for employees, workers, contractors and volunteers and that I have read and understood it.

Signature ……

Date ……

Job Title ……