# DATA PROTECTION POLICY
# GDPR COMPLIANT

## Introduction

The Practice complies with the legal obligations of the Data Protection Act 2018 (the '2018 Act') and the EU General Data Protection Regulation ('GDPR'). The Practice gathers and uses data about workers, employees, and consultants, both to manage our relationships with these individuals and while conducting our business.

This Data Protection Policy applies to all patients, current and former employees, workers, volunteers, consultants, and apprentices ('data subjects'). Data relating to anyone other than a patient will be referred to in this policy as "Staff".

The Practice is a 'data controller' for the purposes of these individuals' personal data and is responsible for determining the purpose and means of the processing of that data.

## Responsibility

This policy will be maintained by the Practice Manager

At Sefton Park MC the role of the data controller is to ensure that data is processed in accordance with Article 5 of the Regulation. The Data Controller is also the Caldicott Guardian at Sefton Park MC and is Mr Simon Turton. They should be able to demonstrate compliance and is responsible for making sure data is dealt with in accordance with the legislation (see later detailed list of tasks).

## Data Processing

Data processors are responsible for the processing of personal data on behalf of the data controller. Processors must ensure that processing is lawful in accordance with this policy.

At Sefton Park MC all staff are classed as data processors as their individual roles will require them to access and process personal data. The Practice Manager will however assume overall day to day supervision of data processing and access issues.

In line with our Records Retention Policy and Computer and Data Security Procedure the Practice has measures in place to protect the security of individuals' data. Policies are available on the Intranet/Shared Drive

The Practice will retain data in accordance with our Records Retention Policy . A copy of this policy is also on the Intranet/Shared Drive. This data will only be held for as long as is necessary for the purposes it has been collected.

This policy has been created to be fully compliant with GDPR and the 2018 Act. Where any conflict arises between those laws and this policy, the Practice will comply with the 2018 Act and the GDPR.

This policy is separate from data subjects' contracts of employment (or contract for services) and can be amended by the Practice at any time.

## Data Protection Principles

The Practice processes personal data in accordance with the six Data Protection Principles for GDPR identified by the ICO, which means it will:

- Be adequate, relevant, and limited to what is necessary for the purposes for which it is processed.
- Be processed fairly, lawfully, and transparently.
- Be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay.
- Be collected and processed only for specified, explicit and legitimate purposes.
- Not be kept for longer than is necessary for the purposes for which it is processed; and
- Be processed securely.

## Personal Data

'Personal data' is defined as information relating to a living person ('data subject') that can be used to identify them on its own, OR in combination with other information likely to be collected by the Practice. This applies whether the information is stored physically, electronically, or in any other format.

It does not include anonymised data but does include any expression of opinion about the person, or any indication of the intentions of the Practice or others, in respect to that individual.

Personal data might be provided to the Practice by the individual, or someone else (such as a previous employer or their GP), or it could be created by the Practice. It could be provided or created as part of the recruitment process; during the contract of employment (or services); or after its termination.

In addition to all the clinical information collected by the Practice we will collect and use the following specific types of personal data about staff and anyone else working at the practice:

- Contact details and date of birth.
- Recruitment information e.g., application form, CV, references, qualifications etc.
- Emergency contact details.

- Gender, marital status, and family status.
- Information regarding their contract of employment (or services) e.g., start and end dates of employment; working hours; role; location; pension; benefits; holiday entitlement; and salary (including details of previous remuneration).
- Bank details and information in relation to tax status, including National Insurance number.
- Information relating to disciplinary or grievance investigations and proceedings involving them (whether they were the main subject of those proceedings).
- Electronic information in relation to their use of IT systems/SMART cards/telephone systems.
- Identification documents e.g., passport; information in relation to immigration status; driving licence; and right to work for the Practice.
- Information relating to an employee's performance and behaviour at work.
- Images (whether captured on CCTV, by photograph or video).
- Training records.
- Records of qualifications and registration relevant to their employment or work at the practice
- Any other category of personal data which we may notify personnel of from time to time.

## Special Categories of Personal Data

These comprise personal data consisting of information relating to:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetic or biometric data.
- Health.
- Sex life and sexual orientation; and  Criminal convictions and offences.

The Practice may hold and use any of these special categories of personal data in accordance with the law.

## Processing Personal Data

'Processing' means any operation which is performed on personal data such as:

- Disclosure by transmission, dissemination or otherwise making available.
- Alignment or combination.
- Collection, recording, organisation, structuring or storage (e.g., within a filing system).
- Adaption or alteration.
- Retrieval, consultation, or use; and
- Restriction, destruction, or erasure.

The Practice will process individuals' personal data (including special categories of personal data) in accordance with the obligations prescribed under the 2018 Act, including:

- Performing the contract of employment (or services) between the Practice and the individual.
- Complying with any legal obligation; or.
- If it is necessary for the Practice's legitimate interests (or for the legitimate interests of someone else). The Practice can only do this in circumstances where the individual's interests and rights do not override those of the Practice (or their own). Individuals have the right to challenge the Practice's legitimate interests and request that this processing be halted.

The Practice may process individuals' personal data for these purposes without your knowledge or consent. The Practice will not use staff personal data for an unrelated purpose without informing you about it and the legal basis for processing it.

Please note that if individuals opt not to provide the Practice with some personal data, the Practice may be unable to carry out certain parts of the contract between us, e.g., the Practice needs staff members' bank account details to pay them.

## When the Practice Might Process Staff Personal Data

The Practice is required to process individuals' personal data in various situations during their recruitment, employment (or engagement) and even following termination of their employment (or engagement) for reasons including but not limited to:

- Deciding how much to pay staff, and other terms of their contract with the Practice.
- Ensuring they have the legal right to work for the Practice.
- Carrying out the contract between the Practice and the individual including, where relevant, its termination.
- Carrying out a disciplinary or grievance investigation or procedure in relation to them or someone else.

- Monitoring and protecting the security (including network security) of the Practice, of the individual, other staff, patients, and others.
- Paying tax and national insurance.
- Providing a reference upon request from another employer.
- Preventing and detecting fraud or other criminal offences.
- Processing pension and sick pay information
- To fulfil contractual requirements imposed by NHSE e.g., the Workforce Census
- Any other reason, which we may notify you of from time to time.

The Practice may process special categories of personal data to use information in relation to:

- race, ethnic origin, religion, sexual orientation, or gender to monitor equal opportunities.
- sickness absence, health, and medical conditions to monitor staff absence, assess staff fitness for work, to pay staff benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after health and safety.

The Practice will not take automated decisions about staff using personal data or use profiling except that in some circumstances patient information may be processed in this way to maximise the benefits of diagnosis and treatment.

The Practice will only process special categories of individuals' personal data in certain situations in accordance with the law e.g., with their explicit consent. If the Practice requests consent to process a special category of an individuals' personal data, the reasons for the request will be explained. Individuals do not need to consent and can withdraw consent later if they choose by contacting the Caldicott Guardian – Simon Turton

The Practice does not need consent to process special categories of staff or patient personal data when it is processed it for the following purposes:

- Where it is necessary for carrying out rights and obligations under employment law.
- Where it is necessary to protect individuals' vital interests or those of another person where one or both parties are physically or legally incapable of giving consent.
- Where the individual has made the data public.
- Where processing is necessary for the establishment, exercise, or defence of legal claims; and
- Where processing is necessary for the purposes of treatment, occupational medicine or for the assessment of an individuals' working capacity.

All employment checks, including those for criminal records, will be carried out in line with the guidance from NHS Employers, available at: www.nhsemployers.org/your-workforce/recruit/employment-checks/criminal-record-check

## Sharing Personal Data

Sometimes the Practice might share staff personal data with group companies or our contractors and agents to carry out our obligations under our contract with them or for our legitimate interests such as with Occupational Health or legal services. Patient data will not be shared with any individual companies other than as required by our NHS contract or any national data collection programme and no data will be provided to any company without express consent of the patient or their Parent/Attorney/Guardian.

We will always require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

The Practice will not send any personal data outside the European Economic Area without express consent or in compliance with any legislation in force at that time.

## Processing Personal Data for the Practice

All staff who work for, or on behalf of, the Practice have responsibility for ensuring data is collected, stored, and handled appropriately, in line with this Data Protection policy and all other policies.

The Practice's Caldicott Guardian and Practice Manager are responsible for reviewing this policy and updating the Partners on the Practice's responsibilities for data protection, and any risks in relation to the processing of data. Any questions related to this policy or data protection should be directed to them.

All members of staff must follow these rules:

- Staff must only access personal data covered by this policy if needed for purposes necessary to their job, or on behalf of the Practice, and only if they are authorised to do so. The data must only be utilised for the specified lawful purpose for which it was obtained.
- Personal data must be kept secure and not shared with unauthorised people.
- Personal data that is accessed, stored, and collected for working purposes must be regularly reviewed and updated. This includes informing the Practice of changes to personal contact details.
- Do not make unnecessary copies of personal data. Any unused copies must be kept safe before being securely disposed of.
- Use strong passwords and lock computer screens when not at your workstation.
- Where suitable, anonymise data or use separate keys/codes so that the data subject cannot be identified.

- Do not save personal data to personal computers or other devices.
- Personal data should never be transferred outside the European Economic Area except to comply with the law and with lawful authorisation .
- Lock drawers and filing cabinets and do not leave paper with personal data unattended.
- Do not remove personal data from the Practice's premises without authorisation from your line manager or Caldicott Guardian.
- Personal data should be shredded and securely disposed of when it is no longer needed.

Please contact our Caldicott Guardian/Practice Manager if you have any questions about data protection, or if you become aware of any potential improvements or vulnerabilities in data protection or data security that the Practice can improve upon.

Any deliberate or negligent breach of this policy may result in disciplinary action being taken in accordance with the Practice's Disciplinary Procedure.

It is a criminal offence to conceal or destroy personal data which is part of a Subject Access Request. This conduct would be regarded as gross misconduct under the Practice's Disciplinary Procedure , which could result in dismissal.