# Data Protection Policy (GDPR)

## 1. ABOUT THIS POLICY

1.1 **St Clair Healthcare Limited** ("the Company") is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out our commitment to data protection, and individual's rights and obligations in relation to personal data.

1.2 This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees, referred to as personal data. This policy does not apply to the personal data of clients or other personal data processed for business purposes.

1.3 This policy does not form part of an employee's contract of employment and may be amended at any time without prior notice.

1.4 If you consider that the policy has not been followed in respect of either your own personal data or that of others, you should raise the matter with your Manager.

## 2. DEFINITIONS

2.1 **"Personal data"** is any information that relates to an individual who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.

2.2 **"Special categories of personal data"** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

2.3 **"Criminal records data"** means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

## 3. DATA PROTECTION PRINCIPLES

3.1 The Company processes personal data in accordance with the following data protection principles:

- We process personal data lawfully, fairly and in a transparent manner.
- We collect personal data only for specified, explicit and legitimate purposes.
- We process personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- We keep accurate personal data and take all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- We keep personal data only for the period necessary for processing.

- We adopt appropriate measures to make sure that personal data is secure and protected against unauthorised or unlawful processing, accidental loss, destruction or damage.

3.2 We inform individuals of the reasons for processing their personal data, how we use such data and the legal basis for processing in the Company's privacy notices. We will not process personal data of individuals for other reasons.

3.3 We will update personal data promptly if an individual advises that his/her information has changed or is inaccurate.

3.4 Personal data gathered during the employment, worker, contractor or volunteer relationship, or apprenticeship or internship, is held in the individual's personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which the Company holds personal data are contained in its privacy notices to individuals.

3.5 We keep a record of our processing activities in respect of personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

## 4. INDIVIDUAL RIGHTS

4.1 As a data subject, individuals have a number of rights in relation to their personal data.

4.2 Individuals have the right to make a subject access request. If an individual makes a subject access request, the Company will tell him/her:

- whether or not his/her data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom his/her data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long his/her personal data is stored (or how that period is decided);
- his/her rights to rectification or erasure of data, or to restrict or object to processing;
- his/her right to complain to the Information Commissioner if he/she thinks the organisation has failed to comply with his/her data protection rights; and
- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

4.3 We will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless he/she agrees otherwise.

4.4 If the individual wants additional copies, we will charge a fee, which will be based on the administrative cost to the Company of providing the additional copies.

4.5 To make a subject access request, the individual should send their request to the Data Protection Officer. In some cases, the Company may need to ask for proof of identification before the request can be processed. We will inform the individual if we need to verify his/her identity and the documents we require.

4.6 The Company will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the Company processes large amounts of the individual's data, we may respond within three months of the date the request is received. We will write to the individual within one month of receiving the original request to tell him/her if this is the case.

4.7 If a subject access request is manifestly unfounded or excessive, the Company is not obliged to comply with it. Alternatively, the Company can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the Company has already responded. If an individual submits a request that is unfounded or excessive, we will notify him/her that this is the case and whether or not we will respond to it.

## 5. OTHER RIGHTS

5.1 Individuals have a number of other rights in relation to their personal data. They can require the Company to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data

5.2 To ask the Company to take any of these steps, the individual should send the request to their Line Manager.

## 6. DATA SECURITY

6.1 We take the security of personal data seriously. We have internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

6.2 Where the Company engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, and are under a duty of

confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

## 7. IMPACT ASSESSMENTS

7.1 Some of the processing that the Company carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, we will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

## 8. DATA BREACHES

8.1 If the Company discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. We will record all data breaches regardless of their effect.

8.2 If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

## 9. INTERNATIONAL DATA TRANSFERS

9.1 Personal data may be transferred to countries outside the EEA for references purposes. Data is transferred outside the EEA on the basis of compliance with this policy.

## 10. INDIVIDUAL RESPONSIBILITIES

10.1 Individuals are responsible for helping the Company keep their personal data up to date. Individuals should let us know if data provided to us changes, for example if an individual moves to a new house or changes his/her bank details.

10.2 Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, the Company relies on individuals to help meet our data protection obligations to staff, customers and clients.

10.3 Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- to not disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;

- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- to not remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- to not store personal data on local drives or on personal devices that are used for work purposes.

10.4 Further details about the Company's security procedures can be found in our Data Security policy.

10.5 Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under our Disciplinary Procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to summary dismissal.