THE GEORGE COOPER PHYSIOTHERAPY AND SPORTS INJURY CLINIC
27 Cambridge Road, Stansted, Essex, CM24 8BX
www.gcphysiotherapy.co.uk
Email: info@gcphysiotherapy.co.uk

GDPR DEPARTMENTAL POLICY:

In order to be GDPR compliant from the 25th May 2018 we have reviewed our data protection policy and formulated the following:

CONTENTS:

1. POLICY

The George Cooper Physiotherapy and Sports Injury Clinic has a clear policy on confidentiality & GDPR that is essential to protect the privacy of individuals – both clients & staff to ensure a high standard of practice at all times. This policy provides a guidance framework within which staff must exercise professional judgement where necessary in consultation with the clinic managers as appropriate. The company's policy on confidentiality & GDPR will be explained to employees as part of their induction. The policy is also available to service users on request.

2. GDPR & Access to Records

Data protection means that those who decide how & why personal data is processed (known as data controllers) must comply with the rules of good information handling, known as the data protection principles. As employers we are the data controller- The George Cooper Physiotherapy and Sports Injury Clinic. Those about whom data is processed (data subjects) – staff and clients are also provided with a number of rights which they may use to access certain information about them, as well as control the way in which it is processed in some cases. The main legislation governing GDPR is The Data Protection Act 1998(DPA), which came into force on the 1st March 2000. The DPA applies to all workers including employees and former job applicants.

There are 8 principles put in place by the DPA and subsequent amendments which specify that data must be:

- Fairly and lawfully processed for limited purposes

- Adequate, relevant and not excessive
- Accurate
- Not kept for longer than is necessary
- Processed in line with your rights
- Secure
- Not transferred to countries outside the EU without adequate protection

The definition of data falling within the DPA is complex. It includes information:

- Which is personal data relating to a living individual, and
- Includes any expression of opinion about the individual and/or
- Includes an indication of the intentions of the data controller or any other person in respect of the individual.

The individual must be identified from the data.

The DPA applies to personal data in:

- Computerised format
- Manual format
- Any other format as long as the data is in a system that allows the information to be readily accessible.

All files relating to service users and employees will be kept in locked filing cabinets or on a computerised filing system which is security protected. Access to these files will be limited to key members of staff who need the information contained within them in order to carry out their jobs.

Individuals may request copies of their file information (subject access request). All requests must be made in writing to the employer. These will be provided within one month from receiving the request unless extensive then an extension may be requested.

The address details and telephone numbers of employees and service users should never be given out to any third party who may contact the organisation. In situations where there is a request for address or telephone details a message should be taken and the individual concerned contacted.

Information relating to individuals employment with the organisation such as absence records and disciplinary information will be considered highly confidential and will be processed and stored in line with the DPA guidelines

On the termination of an employment relationship, The George Cooper Physiotherapy and Sports Injury Clinic will retain personnel records for as long as there is a real business need. E.g. to provide a reference or be able to defend any future claims.

Reporting directly to the UK parliament the information commissioner's office is a UK independent supervisory authority which insures that organisations which process data does so in compliance with the DPA, Free of Information Act 2000 the privacy and electronic communications regulations 2003 and The Environmental

Informational Regulations 2004. The website of The ICO is the most comprehensive source for guidance on GDPR and guidance can be found at:

http://ico.org.uk

3 Basic Principles of Client Confidentiality

Information relating to service users must be treated with respect at all times.

Where written records are absolutely necessary, recordings must be accurate, concise, factual and clear. They must contain the minimum amount of information that is necessary for the purpose intended.

Clients personal circumstances of any type are not to be relayed or discussed with anyone either inside or outside of George Cooper Physiotherapy and Sports Injury Clinic unless we are instructed otherwise by the client concerned. Consent should always be sought in situations where it is necessary to pass on information to enable service delivery to the individual concerned.

Information should only ever be passed on in cases where there is a legitimate need to know and only relevant and necessary information should be revealed e.g. reports to referrers or onward referrals to a tertiary service. However there are certain situations where information will need to be shared even if this is against the wishes of the service user. This includes situations where:

- A clients life is at risk
- Other individuals life's are at risk
- It is a requirement of a court order
- It is a requirement of law
- Where there is a child protection/vulnerable adult issue

There may also be occasions where there is a public interest justification for the disclosure of information including:

- Public accountability and monitoring purposes
- Where there is a serious risk to public health
- The prevention, detection, or prosecution of serious crime

Any requests for information from an external agency should always be discussed with the employer and fully documented.

4. Confidentiality in the workplace

Personal details of any employee must not be disclosed without their consent.

- All staff should ensure that documents:
- Are not left lying unattended on desks
- Are not left open and visible on computer screens
- Are filed away securely after use

Staff, who are dealing with ongoing queries that contain confidential client information must ensure that all details are stored away appropriately at the end of the day.

All confidential records are to be stored in a locked filing cabinet on the premises of The George Cooper Physiotherapy and Sports Injury Clinic. The key will be held by the employer in a secure place.

All information that does not need to be stored will be shredded and disposed of appropriately

Any loss of sensitive documents should be reported with immediate effect to the employer. If a data breach occurs, the ICO would be notified where feasible within 72 hours, unless the breach is unlikely to result in risk to individuals.

5. General Security Procedures

All employees should adhere to the following security measures at all times:

- Office doors should be locked at the end of the day and at all times when the clinic is empty
- All visitors to the office must be accompanied at all times by a member of staff
- Phones should be password protected
- Computers must be password protected and have up to date anti-virus and firewalls
- Emails should be sent securely
- Social Media should have no personal identifiers
- If a testimonial is received consent must be gained to utilise this for advertising purposes
- Written consent must be obtained for photographs or videos as per our consent form
- Anything sent by post should be sent recorded and signed for where possible and titled private and confidential
- Complaints received will be dealt with confidentially and promptly by the employer and a record stored in patient notes

6. Data Processors

A data processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. E.g. Cliniko, Microsoft Office, IT Consultants, Accountants, Joint note holders (nurseries/nursing homes)

GDPR will be met by their terms and conditions when they set up their services. If they breach data they will be liable to be investigated by The ICO.

7. Data Protection Officers (DPO)

Data protection officers are responsible for overseeing data protection strategies and implementations to ensure compliance with GDPR. As a small business it is not possible to employ a separate DPO therefore the appointed officers at The George Cooper Physiotherapy and Sports Injury Clinic are: George Cooper and Sylvia Ringhofer.

8. Breaches of GDPR and Confidentiality

Any suspected breaches of confidentiality will be taken seriously and investigated thoroughly in line with the disciplinary policy and procedure. If a breach is found to have taken place this may constitute gross misconduct and following a disciplinary hearing may result in dismissal.

By adhering to the above policy we are minimising the risk of a data breach to the best of our abilities.

9. Signatory

……
Print Name

……. ……..
Signature on behalf of Date
The George Cooper Physiotherapy and Sports Injury Clinic

……
Print Name

……. ……..
Signature on behalf of Date
The George Cooper Physiotherapy and Sports Injury Clinic