Melanie Arazi BSc Hons MCSP HCPC APCP

Highly Specialist Paediatric Physiotherapist

www.childrensphysioclinic.co.uk

The Children's Physiotherapy Clinic Data Protection and Privacy Policy 2018

Table of Contents:

4.6 Data Quality

4.7 Data Protection

4.7.1 Data Security

4.7.2 Responsibilities

4.7.3 Risks

4.7.4 General Guidelines

4.7.5 Data at Rest

4.7.6 Data in Transit

4.7.7 Data Transfers

4.8 Data Retention

4.9 Data Destruction

4.10 Rights of Data Subjects

4.10.1 Data Subject Access Requests

4.10.2 Data Subject Erasure and Rectification Requests

4.11 Data Protection Training

4.12 Complaints Handling

4.13 Breach Reporting

1. Introduction

1. Introduction and Contact Details

The Children's Physiotherapy Clinic needs to collect and process personal data, including special category data, about individuals in order to provide an effective service.

We are committed to protecting your rights and privacy and as such adhere to strict data protection guidelines as set out in this document. We are a data controller and are responsible for your personal data. By providing us with your and your children's data, you warrant to us that you are over 13 years of age.

This Data Protection and Privacy Policy ("Policy") describes how your personal data is collected, processed and stored to meet our own data protection standards and to comply with current EU and UK legislation.

This Policy ensures that we:

- comply with current data protection legislation and adopt good practice.
- protects your rights.
- are transparent about how we store and process your data.
- protect ourselves and you from the risks of a data breach.

Our full contact details are:

Full name of Legal Entity: Melanie Arazi trading as The Children's Physiotherapy Clinic

Email address: melanie@childrensphysioclinic.co.uk

Postal address: 30 Lodge Avenue, Elstree, Herts, WD6 3ND

Please note that we may communicate with you / the patient / the patient's carer / the patient's medical representatives (with prior permission in the case of the latter) by electronic means (e.g. email, text message) or in hard copy letter form as well as by telephone.

2. Scope

This policy applies to all employees of The Children's Physiotherapy Clinic (as defined below), in relation to the processing of any personal data relating to current, past and prospective clients and employees of The Children's Physiotherapy Clinic.

3. Definitions

***Client**:* Any past, current or prospective client of The Children's Physiotherapy Clinic.

Consent: Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data Processing: Any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Subject*:* The identified or identifiable natural person to which the data refers.

Employee: An individual who works part-time or full-time for The Children's Physiotherapy Clinic under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. Includes temporary employees and independent contractors.

Encryption: The process of converting information or data into code, to prevent unauthorised access.

Information Commissioner's Office (ICO): The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Personal Data: Any information which relates to an identified or identifiable individual, not including anonymised data.

Personal Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Special Categories of Data: Personal data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

Third Party*:* An external organisation with which The Children's Physiotherapy Clinic conducts business and is also authorised to, under the direct authority of The Children's Physiotherapy Clinic, process the Personal Data of The Children's Physiotherapy Clinic's clients.

4. Policy

4.1 Relevant Legislation

Please follow these links for access to data protection rules, regulations and legislation relevant to this Policy:

Data Protection Bill

https://publications.parliament.uk/pa/bills/cbill/2017-2019/0153/18153.pdf

General Data Protection Regulation ("GDPR")

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Data Protection Act 1998

http://www.legislation.gov.uk/ukpga/1998/29/contents

4.2 Data Protection Principles

We are committed to data protection and to following the data protection principles found in applicable rules, regulations and legislations. As such the policies and procedures outlined within this document have been designed to ensure that we are able to collect, process, store and dispose of Personal Data relating to its Data Subjects in a legal and fair manner.

In compiling this Policy we have adhered to the eight principles governing the use of Personal Data as set out in The Data Protection Act 1998. These principles are:

1. *Personal data shall be processed fairly and lawfully and shall not be processed unless— (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.*
2. *Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.*
3. *Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.*
4. *Personal data shall be accurate and, where necessary, kept up to date.*
5. *Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.*
6. *Personal data shall be processed in accordance with the rights of data subjects under this Act.*
7. *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*
8. *Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.*

We have also adhered to Article 5 of the GDPR which sets out an updated version of the above principles:

1. *Lawfulness, fairness and transparency: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.*
2. *Purpose limitation: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.*

3. *Data minimisation: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.*
4. *Accuracy: Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.*
5. *Storage limitation: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.*
6. *Integrity and confidentiality: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.*
7. *Accountability: The controller shall be responsible for, and be able to demonstrate compliance with, the above six principles.*

4.3 Privacy by Design

To incorporate privacy by design, we will ensure that all data protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes.

4.4 Data Collection

4.4.1 Data Sources

We will collect and process certain types of data about you, such as:

- Identity Data, which may include your first name, maiden name, last name, username, marital status, title, date of birth and gender
- Contact Data, such as your billing address, delivery address, email address and telephone numbers
- Medical Data, such as your weight, height and medical history
- Financial Data, such as your bank account and payment card details
- Transaction Data, such as details about payments between us and other details of purchases made by you
- Technical Data, such as internet protocol addresses, browser type and version, browser plug-in types and versions, time zone setting and location, operating system and platform and other technology on the devices you use to access The Children's Physiotherapy Clinic's website
- Profile Data, such as orders, your interests, preferences, feedback and survey responses

- Usage Data, such as information about how you use The Children's Physiotherapy Clinic's website, products and services
- Marketing and Communications Data, such as your preferences in receiving marketing communications from us and from a Third Party and your communication preferences

Data will be collected through a variety of different methods including:

- Direct interactions
- Automated technologies or interactions
- Third parties or publicly available sources

Personal Data collected by us will only be collected from the Data Subject unless one of the following apply:

- The nature of the contract necessitates collection of the Personal Data from other persons or bodies.
- The Data Subject has consented to the collection of the Personal Data from other persons or bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person

If Personal Data is collected from someone other than the Data Subject, we will inform the Data Subject of the collection unless one of the following apply:

- The Data Subject has received the required information by other means.
- The information must remain confidential due to a professional secrecy obligation
- A national law expressly provides for the collection, processing or transfer of the Personal Data.

Where it has been determined that notification to a Data Subject is required, notification will occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the Personal Data
- At the time of first communication if used for communication with the Data Subject
- At the time of disclosure if disclosed to another recipient

4.4.2 Data Subject Consent

Article 7 of the GDPR sets out the conditions for lawfully processing Personal Data based on consent of the Data Subject.

We will collect Personal Data only by lawful and fair means and with the knowledge and Consent of the individual concerned. We are committed to seeking such Consent where a need exists to request and receive the Consent of an individual prior to the collection, use or disclosure of their Personal Data.

We have established a system for obtaining and documenting Data Subject Consent for the collection, processing, and/or transfer of their Personal Data, via our "Physiotherapy Consent Form for Data Processing". We have ensured that the request for Consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language. We have ensured that the Consent is freely given and is not based on a contract that is conditional to the processing of Personal Data that is unnecessary for the performance of that contract.

We have established a system to document the date, method and content of the Consent attained form the Data Subjects, as well as the validity, scope, and volition of the Consent given. We have provided a simple method for a Data Subject to withdraw their consent at any time and will notify the Data Subject of this in writing at the time of obtaining Consent.

4.4.3 Data Subject Notification

We are committed to providing Data Subjects with information as to the purpose and lawful basis of the processing of their Personal Data. When we ask the Data Subject to give Consent to the processing of Personal Data and when any Personal Data is collected from the Data Subject, all appropriate disclosures will be made in writing, unless one of the following apply:

- The Data Subject already has the information
- A legal exemption applies to the requirements for disclosure and/or Consent.

The data notification will be given in writing and a record kept by us.

4.4.4 Website Consent and Cookies

Consent to processing of information collected via our website will be gained via an opt-in tick box which will clearly set out the lawful basis for collection of data.

Cookies are small text files that are downloaded to your computer or mobile device. Cookies do not harm your computer. Cookies help us to provide you with a good user experience when you browse our website. Cookies are not used to collect or record information like your name, address or any of your personal details. Cookies are used on our website to collect statistics about how visitors interact with the website; which search engine they used to find the site and record statistics such as your browser, IP address, general location and operating system and type of device used to view our site. These details help us to improve

on how we manage and maintain the website to give you the best possible visitor experience.

Most web browsers accept the use of cookies. Unless you have adjusted your browser settings so that cookies are not allowed, cookies will be set when you first access the site and accept the "OK Cookies" prompt at the top of the screen.

By browsing our website, you understand that cookies will be collected from you.

The website may include links to Third Party websites, plug-ins and applications, which may in turn enable Third Parties to collect or share data about you. We do not control these Third Party websites and are not responsible for their privacy statements. It is important to read the Third Party's own privacy and cookie policy.

4.5 Data Use

4.5.1 Data Processing

We are committed to processing data in a lawful, fair and transparent manner. As such we and our employees will adhere to the guidelines set out in this Policy.

In accordance with Article 6 of the GDPR Article 6, at least one of the following conditions must be met for the processing of personal information to have a lawful basis:

a) *the data subject has given consent to the processing of his or her personal data for one or more specific purposes.*
b) *processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.*
c) *processing is necessary for compliance with a legal obligation to which the controller is subject.*
d) *processing is necessary in order to protect the vital interests of the data subject or of another natural person.*
e) *processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.*
f) *processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*

We will only process data when (a) the Data Subject has given Consent to Data Processing for one or more specific purposes and/or b) processing is necessary for the performance of a contract to which the Data Subject is party or to take steps at the request of the Data Subject prior to entering into a contract.

We will only use your data for the purposes for which it was collected, unless it is reasonably considered necessary to use it for another reason and that reason is compatible with the

original purpose. If you wish to find out more about how the processing of the new purpose is compatible with the original purpose, please email melanie@childrensphysioclinic.co.uk.

If we need to use your data for a purpose which is unrelated to the original purpose for which the data was collected, we will notify you and explain our reasoning for doing so.

We may have to share your data with Third Parties, such as service providers who provide IT and system administration services, professional advisers, HM Revenue & Customs and regulators/authorities. We require such Third Parties to process your data for specified purposes and in accordance with our instructions and to respect the security of your data and to treat it in accordance with the law.

4.5.2 Special Categories of Data

Additionally, as regards Special Categories of Data, Article 9 of the GDPR sets out a further set of conditions, of which at least one must be fulfilled for the processing of Special Categories of Data to be lawful:

a) *the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.*
b) *processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.*
c) *processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;*
d) *processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.*
e) *processing relates to personal data which are manifestly made public by the data subject;*
f) *processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;*
g) *processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;*
h) *processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;*
i) *processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union*

or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

j) *processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.*

We will process Special Categories of Data when the conditions set out at (a), (e), (f) or (h) above apply.

Article 10 of the Data Protection Bill sets out further safeguards which need to be satisfied for the processing of Special Category Data to be lawful under UK law. We will use point (h) (health and social care) as a lawful basis for processing Special Category Data.

4.5.3 Children's Data

Pursuant to the Data Protection Bill children under 13 years of age are unable to consent to the processing of their Personal Data under UK law, and as such, we will obtain consent from the legal parent or guardian of the underage Data Subject.

4.6 Data Quality

We will adopt all necessary measures to ensure that the Personal Data we collect and process is complete and accurate in the first instance and is updated to reflect the current situation of the Data Subject. We take responsibility to correct all Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification.

We will keep Personal Data only for the period necessary to satisfy the permitted uses or applicable statutory retention period and will ensure the removal of Personal Data if in violation of any of the data protection principles or if the Personal Data is no longer required.

We will restrict rather than delete Personal Data, insofar as a law prohibits erasure or the Data Subject disputes that their Personal Data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

4.7 Data Protection

4.7.1 Data Security

We are committed to safe guarding the rights and privacy of our Clients and as such adhere to the following principles of data protection and security in order to minimise the risk of a Personal Data Breach.

4.7.2 Responsibilities

Each of our Employees has responsibility for ensuring data is collected, stored and handled appropriately.

4.7.3 Risks

Information security and Personal Data Breaches may cause real harm and distress to the individuals they affect. We process sensitive Personal Data about individuals and as such are required to ensure we have appropriate safeguards in place to maintain the security and protection of the data we hold in order to protect the rights and privacy of Data Subjects. A Personal Data Breach comes with the following risks which the safeguards set out in this policy aim to minimise:

- Risk of breaching patient confidentiality.
- Risk of harm and/or damage to individuals as a result of dissemination and/or loss of Personal Data.
- Risk of damage to organisation's reputation.

4.7.4 General Guidelines

We follow the following guidelines:

- Person-identifiable or confidential information is effectively protected against improper disclosure when it is received, stored, transmitted or disposed of.
- Access to person-identifiable or confidential information is on a need-to-know basis.
- Disclosure of person-identifiable or confidential information is limited to that purpose for which it is required.
- Recipients of disclosed information respect that it is given to them in confidence.
- Person-identifiable information, wherever possible, is anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data.
- We provide training to all Employees to help them understand their responsibilities when handling data.
- Personal data is not disclosed to unauthorised people, either within the company or externally.
- Data is regularly reviewed and updated if it is found to be out of date. If no longer required, it is deleted and disposed of via approved channels.

- Our Employees should always request more information if they are unsure about any aspect of data protection.

4.7.5 Data at Rest

These rules describe how and where your data is safely stored.

When data is stored in a paper record format, it is kept in a secure place where unauthorised people cannot access it:

- All records containing person-identifiable or confidential information is stored in a designated locked cabinet or safe.
- Unwanted paper records containing person-identifiable or confidential information is shredded and disposed of securely when no longer required.

When data is stored electronically, it is protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data is only stored on designated encrypted drives and servers and is only uploaded to approved cloud computing services.
- All servers, and devices, containing or used to access Personal Data, is protected by approved security software and a firewall.
- Data is never saved directly to unencrypted laptops or other devices such as tablets or smart phones (save for via secure, approved cloud computing services).
- Data is protected by strong passwords which are changed frequently and never shared even amongst employees.
- Passwords are a minimum of eight characters, and contain at least one number, a mixture of capital and lower-case letters and a special character. Passwords are completely random and not contain easy to guess words or number sequences.
- Servers and devices containing Personal Data are sited in a secure location, such as a safe or locked cabinet to which unauthorised people do not have access.
- Data is backed up frequently. Those backups are tested regularly to ensure that the data is protected against accidental deletion or corruption.

4.7.6 Data in Transit

- To ensure safety of confidential information whilst in transit, Personal Data about any past, present or prospective Client is safeguarded at all times and never be left in an unsecure location.
- When physically transporting Personal Data, whether in paper or electronic form, our Employees ensure that it is on their person at all times or left in a secure, lockable

location, that unauthorised people do not have access to.

- Data is subject to encryption before being transferred electronically and is transferred via approved email software.
- Personal Data is never transferred outside of the European Economic Area ("EEA") unless specific safeguards have been put in place in line with current legislation. Some of our Third Party providers may be based outside of the EEA so their processing of your Personal Data may involve a transfer of data outside the EEA. If this applies, we will ensure similar degrees of security of data to the extent this is within our reasonable control.

4.7.7. Data Transfers/Disclosure

We will consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed. Information can be disclosed:

1. With consent of the Data Subject.
2. When effectively anonymised.
3. When the information is required by law or under a court order.

4.8 Data Retention

We will not keep Personal Data records for longer than necessary in relation to the purposes for which it was originally collected and provided this is in keeping with minimum retention periods for health records relating to children and young people (such records must be retained until the patient's 25th birthday or 26th if the young person was 17 at conclusion of treatment, or 3 years after death).

4.9 Data Destruction

All Personal Data held by us will be destroyed once it has been established that there is no further need to retain the data, either for the use for which it was originally obtained, nor for legal or statutory purposes, and the minimum retention period as set out by the ICO has passed.

We will ensure that all data is destroyed fully and completely so that there is no risk of a Personal Data Breach. This includes but is not limited to paper records, information stored on encrypted drives and other hardware.

4.10 Rights of Data Subjects

Pursuant to Article 12 of the GDPR, Data Subjects have increased rights to access, rectify and erase their Personal Data, held by us. We will ensure that we adhere to these rights.

In addition, we will ensure that Data Subjects are notified that requests for data rectification and erasure have been complied with.

4.10.1 Data Subject Access Requests

In accordance with the GDPR, as a Data Subject you have the right of access to Personal Data which has been collected by us. As such we have established a protocol to deal with all Data Subject Access Requests, in accordance with Article 15 of the GDPR.

You will be notified in writing of your rights to request access to any Personal Data processed by us relating to you and/or your child(ren) at the time of consent to the processing of your Personal Data by us. You will will be informed in writing at this time of the relevant protocols that exist to enable you to exercise these rights.

You can request access to the Personal Data which we hold about you or your child by submitting your request in writing, via email to: melanie@childrensphysioclinic.co.uk.

Where your request is found to be valid (see below), we will fulfil your request within 30 days. A further 60-day extension period is available to us in dealing with requests for data that may take more time to respond too. If this is the case, we will inform you of this within 30 days of receiving the original data subject access request.

On receipt of a data subject access request, we will acknowledge receipt of the request and will verify the identity of the person making the request via a phone call to you.

Once your identity has been verified, we will take the following steps:

1. All the data processed about the individual making the request will be collated.
2. If we do not hold any data about you, then this will be communicated to the individual who made the request in writing within 30 days.
3. If we do hold personal data about the individual, then an electronic copy of all the Personal Data processed by us will be sent to the Data Subject via an approved channel.

Any data that is not supplied to you in accordance with the exemptions set out in the GDPR will be explained to you. Any data relating to another Data Subject that cannot be separated from the data will be redacted to avoid breaching the rights of other Data Subjects.

Subject access request responses from us will include the following information:

- Purpose of processing.
- Categories of Personal Data processed.
- Recipients or categories of recipients to whom the data has been or will be disclosed to.
- How long the data will be stored for.
- Existence of the Data Subject's right to rectification, erasure and/or restriction of processing of their Personal Data held by us.
- Informing the Data Subject that they have the right to lodge a complaint if they do not feel their request has been handled effectively.
- The source of the data processed by us (if it was not the Data Subject).

4.10.2 Data Subject Erasure and Rectification and Restriction of Processing Requests

Under Articles 16 - 19 of the GDPR, Data Subjects have the right to request rectification, erasure or restriction of processing of their Personal Data held and processed by us and to be informed by us that their requests have been acted upon:

You will be informed in writing of your rights to request rectification, erasure or to restrict the processing of your Personal Data held by us at the time at which they consent to the processing of your Personal Data by us.

Data Subjects can submit a request for data rectification, erasure or to restrict the processing of their Personal Data, by submitting their request in writing via email to: melanie@childrensphysioclinic.co.uk.

We will acknowledge receipt of any request from a Data Subject and will send a notification regarding the rectification, erasure or restriction of processing of Personal Data that has resulted from the request.

You will not have to pay a fee to access your Personal Data. However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive and may refuse to comply with a request in such circumstances.

4.11 Data Protection Training

Data protection training will be undertaken by all our Employees to ensure familiarity with data protection principles, and such training will be updated every two years, to ensure we remain up to date and familiar with data protection legislation.

4.12 Complaints Handling

In accordance with the GDPR, Data Subjects have the right to submit a complaint to ICO, the UK supervisory authority for data protection issues (*www.ico.org.*uk), if they are not happy with how their data has been collected and used. However, please contact us first if you do have a complaint so that we can try to resolve it for you.

4.13 Breach Reporting

Articles 33-34 of the GDPR address data breaches. In accordance with these provisions and the terms of the Data Protection Bill, in the case of a Personal Data Breach, we will take the steps set out below.

1. Notification of the breach must be made to the ICO within 72 hours (if later than this then an explanation for the delay must also be included).
2. Notification will include:
   (a) a description of the data breach, including (i) the categories of subjects and number of subjects affected by the data breach; and (ii) the categories of records and number of records affected by the data breach.

(b) the name and contact details of the contact point from whom more information can be obtained.
(c) a description of likely consequences of the data breach.
(d) a description of the measures taken to address the Personal Data Breach including where applicable ways to mitigate any adverse effects.

We will inform you that you are affected by a Personal Data Breach and that your Personal Data has been compromised unless an exemption as outlined in the GDPR and Data Protection Bill applies.