**8th May 2018**

**PILATES HEALTH PHYSIOTHERAPY**

---

# Data Protection Policy

---

Pilates Health Physiotherapy

*Move Well ..... Stay Well!*


www.pilates-health.com

info@pilates-health.com

*07789 465383*

*6 High Bois Lane, Chesham Bois, Bucks, HP6 6DG*

# DATA PROTECTION POLICY

In the course of running its day to day business Pilates Health Physiotherapy (PHP) may collect and process information about its clients and staff as well as members of the public such as enquirers and correspondents. Please read the following to understand our practices regarding your personal data. The PHP website **www.pilates-health.com** (our 'Website') contains links to and from other related websites. Please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to these websites.

**PHP may collect and process the following data:**

| Data held | Classification | What it's used for | Protected/managed |
|---|---|---|---|
| **Instructors / Staff** personal data, employment history, education and qualifications, contact details, bank details and record of employment with PHP. | Sensitive Data | Very occasionally, PHP may process information about its staff's health or medical details. PHP processes such employee personal data for ordinary staff administration purposes, including payment and conferring other benefits, training and management. It also collects personal data about prospective candidates in the recruitment process. | Password protected computer and banking software. Bullguard firewall protection along with anti-virus and spyware protection, hardware firewall, encrypted cloud backup.<br><br>Jaguar Consultants privacy policy retained on file |
| **Clients** personal data of its past, present and prospective clients. The personal data held includes clients' health and attendance history, personal and family circumstances, contact details, and may include financial details. | Personal Data | PHP processes such personal data in order to administer classes, to collect payment and to ensure that staff are aware of specific medical issues. PHP holds some information about past clients for archival purposes. We may ask you to complete optional surveys for research purposes. | Password protected computer and banking software. Bullguard firewall protection along with anti-virus and spyware protection, hardware firewall, encrypted cloud backup.<br><br>We may share client data amongst staff, but will not transfer any client data to any third parties without permission unless indicated in this privacy policy. We will never sell member or third party data for the purposes of marketing. |

| | | | |
|---|---|---|---|
| **The public** | Personal Data | PHP may enter into correspondence with members of the public, such as enquirers and correspondents. When it does so, PHP may collect incidental personal data such as contact details and personal circumstances, and process such personal data in order to respond to queries and deal with relevant issues. We may ask you to complete optional surveys for research purposes. | Password protected computer and banking software. Bullguard firewall protection along with anti-virus and spyware protection, hardware firewall, encrypted cloud backup. |
| **Suppliers** PHP processes personal data concerning its suppliers of goods and services, including identifiers such as contact details, financial information and purchase history. | | PHP processes such information in order to purchase goods and services, to pay its suppliers and to maintain its accounts and records. | Password protected computer and banking software. Bullguard firewall protection along with anti-virus and spyware protection, hardware firewall, encrypted cloud backup. |
| **Photographs** | Personal Data | PHP may take photographs at classes for use on the Website or promotional literature. You would be advised in advance of this happening and can choose to opt out. | Images are stored on a password protected computer. Bullguard firewall protection along with anti-virus and spyware protection, hardware firewall, encrypted cloud backup. However, these images may be used in the public domain (website, leaflets) |

## Applicable data protection law:

Data protection law in England and Wales is primarily found in the Data Protection Act 1998 ('**DPA**'). With effect from 25th May 2018, the DPA will be repealed and superseded by the General Data Protection Regulation ('**GDPR**'). The GDPR will be supplemented by the Data Protection Act 2017. In this policy, any reference to the Data Protection Legislation means the DPA, or the GDPR, as supplemented by the Data Protection Act 2017 ('**DPA 17**'), whichever is in force at the time.

The DPA is enforced in England by the Information Commissioner, operating through the Information Commissioner's Office (the '**ICO**'). The ICO publishes guidance on the DPA and has a broad range of powers, including the ability to issue fines of up to £500,000 for breaches. The ICO will enforce the GDPR when it takes effect in May 2018. Under the GDPR, the ICO will have greater powers, including the ability to issue fines of up to 4% of annual turnover, or €20,000,000, (whichever is greater) and to conduct compulsory audits of organisations' data handling practices.

**Key concepts of applicable data protection law**

The Data Protection Legislation relies on a number of key definitions, which are explained below.

'***personal data***' means any information relating to an identified or identifiable natural person (a 'data subject', which is explained in more detail below). An identifiable natural person is one who can be

identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the identity of that natural person.

PHP will hold personal data about its past, present and prospective clients as well as its suppliers. PHP may hold such personal data both in electronic and hard copy format, in records and correspondence.

'***processing***' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing is interpreted very broadly, so that almost all activities organisations carry out in relation to their personal data are captured by the definition.

PHP will generally be deemed to be processing any personal data that it may collect, record, store and/or disclose.

'***controller***' means the natural or legal person, public authority, agency or other body, which determines the purposes and means of the processing of personal data. The Data Protection Legislation applies to controllers, who must comply with its requirements.

PHP will generally be a controller in relation to the personal data of its clients, staff, members of the public such as enquirers, and suppliers.

'***processor***' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Where a controller uses a processor to process personal data on its behalf, the controller must only use a processor that provides sufficient guarantees to ensure that personal data is processed securely, and in accordance with the requirements of the GDPR. Controllers must engage processors by way of a contract incorporating the provisions specified by Article 28 of the GDPR.

PHP will generally be a processor for a variety of purposes; for instance, to store personal data, to send email communications, or to calculate instructor payments.

'***special categories of personal data***' means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic or biometric data, data concerning health (including medical data, and medical records, for example), or concerning an individual's sex life or sexual orientation. Special categories of personal data is the term used in the GDPR which, broadly speaking, replaces the concept of 'sensitive personal data' from the DPA.

The special categories of personal data require a higher standard of care. If a personal data breach (as defined below) occurs that involves the loss of any of the special categories of personal data, the ICO will regard this as a serious breach. The GDPR also requires that personal data relating to criminal convictions and offences is treated with a higher standard of care.

PHP does hold medical records of clients and will ensure the information is handled accordingly.

'***data subject***' means an individual to whom personal data relate. Typically, these are employees, customers, and suppliers.

The categories of data subject whose personal data PHP is likely to process will include clients, instructors, suppliers and members of the public.

‘***personal data breach’*** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

A personal data breach may be accidental, such as a system failure, or loss of an electronic or physical file, or malicious, such as a cyberattack. In the event that PHP suffers a personal data breach, it will take specific steps, explained below in this policy.

## The data protection principles:

The data protection principles are standards which PHP must observe when processing personal data. These principles are as follows:

**Fairness:** Organisations generally cannot process individuals' personal data in a way that an individual would not have reasonably expected. Collecting personal data on the pretext of one purpose and then using it for another, unrelated purpose is unlikely to be fair. PHP will consider whether its uses of personal data would fall within the reasonable expectations of the affected data subjects.

**Transparency:** Organisations must provide certain prescribed information to individuals when processing their personal data, including the organisation's identity, the purposes for which personal data are being processed, or are to be processed, and any third party recipients of the personal data. A complete list of the information that must be provided to data subjects can be found in Articles 13 and 14 of the GDPR. The transparency information must accurately reflect the controller's use of personal data. This is frequently provided by way of a website privacy notice, but may also be provided by way of a disclaimer on a paper form, or a pre-recorded message in the context of recorded telephone calls.

PHP will ensure that its website privacy notice, and any other means by which it makes the transparency information available to data subjects (such as a disclaimer on a paper form) accurately and comprehensively reflect its processing activities.

**Lawfulness:** Organisations must establish at least one of a number of lawful grounds for processing. These lawful grounds are set out in Article 6 of the GDPR and are as follows:

1) The data subject has given his or her **consent** to the processing. Note that to be valid, consent must be freely-given, informed (by way of the transparency notice, explained above) specific, and capable of withdrawal at any time, without detriment to the data subject. Consent must be indicated by way of an unambiguous, positive affirmation by the data subject. Consent cannot be inferred from the absence of an objection, and will not be valid where the data subject does not have a genuine choice.

2) Processing is necessary for the **performance of a contract** to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract.

3) Processing is necessary for **compliance with a legal obligation** to which the controller is subject.

4) Processing is necessary in order to protect the **vital interests of the data subject** or of another person.

5) 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.

6) Processing is necessary for the purposes of **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 the protection of personal data.

**Purpose limitation**

This principle requires that the purposes for which personal data are processed are limited to those purposes specified in the transparency information that has been provided to the affected data subjects, and not processed for any further, incompatible purposes. Any further processing operations for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes are not considered to be incompatible purposes.

PHP will only process personal data it holds for those purposes specified in the website privacy notice, or other such transparency notice.

**Data minimisation**

Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

PHP will only collect the personal data that is strictly necessary for the purpose for which it was collected, and will not collect additional, unnecessary personal data on a 'just in case' basis.

**Accuracy**

Personal data must be kept accurate, and up to date.

PHP will ensure that any requests from data subjects to update their personal data are dealt with promptly, having satisfied itself as to the requester's identity.

**Storage limitation**

Personal data must not be kept for longer than is necessary for the purposes for which the data are processed. The duration for which personal data are stored will be dictated by applicable legal, business or other reasons, such as retention periods driven by tax legislation.

If PHP cannot establish a valid legal, business or other reason for retaining personal data, it will be securely deleted. PHP will specify the periods for which personal data are stored in a record retention policy. After the storage period has expired, personal data should be deleted.

Note that PHP may store some categories of personal data for longer periods where such processing is solely for archiving purposes in the public interest, or historical research purposes. In such cases, PHP will implement appropriate safeguards, such as allowing data subjects to request deletion of some of their personal data.

**Integrity and confidentiality**

Personal data must be processed in a manner that ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

PHP will take appropriate measures that are proportionate to the risk associated with the personal data it holds. Such measures may be technical, such as encryption and password protection of electronic devices

and electronic storage media (e.g. USB drives), or organisational, for example, by operating a layered access policy, appropriate vetting of staff who have access to personal data, conducting appropriate due diligence on any third parties that process personal data on PHP's behalf, and binding them by an appropriate engagement contract. PHP will consider regularly reviewing and testing its security measures.

**Accountability**

Controllers are responsible for compliance with the principles explained above, and must be able to demonstrate compliance.

PHP is able to provide evidence of compliance, for example, by way of a data protection policy and documented data protection reviews.

## Data Breach:

If a data security breach occurs, PHP (as Controller) will notify the breach to the ICO '*without undue delay' and, where feasible, within 72 hrs of the personal data breach occurring*.' However, this notification requirement does not apply where the breach '*is unlikely to result in a risk to the rights and freedoms'* of the individuals concerned.

This notification will include the information specified in Article 33(3) of the GDPR, and where it is not possible to provide all the information at once, it may be provided in phases.

**Reporting breaches to individuals:**

Where a data security breach occurs, and it is likely to result in a 'high risk' to the rights and freedoms of the individuals concerned, PHP must notify the affected individuals 'without undue delay'. Article 34(2) of the GDPR specifies what information must be provided. However, PHP is not required to notify data subjects if:

1) The personal data concerned had been rendered unintelligible (for example, by way of encryption)' or
2) Subsequent measures have been taken by PHP so that there is no longer a high risk to the individuals; or
3) It would involve disproportionate effect to communicate to each affected data subject individually, although where this applies then a general public communication will be made.

PHP will maintain a schedule of data breaches (whether or not notification was made at the time), to comply with Article 33(5) of the GDPR.

**Data protection impact assessments (DPIAs)**

A DPIA consists of a documented consideration and evaluation of the data protection risks arising from a proposed new processing activity, along with recommended mitigation strategies to address the risks.

Under Article 35 of the GDPR, PHP is required to undertake a DPIA "*where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons*"

PHP does not believe that the nature of its processing is such that there is likely to be a high risk to the rights and freedoms of the data subjects whose personal data it holds. As a result, PHP does not believe that it is necessary for it to undertake any DPIAs.

PHP will keep this conclusion under review, including any guidance issued from ICO, or practice in other similar schemes

## Third party processors:

PHP will ensure that it has a written contract which meets the requirements of GDPR in place with each processor it uses. PHP will only use processors that guarantee they will meet the requirements of the GDPR and will protect data subjects' rights.

Before engaging a processor, PHP will check that the processor has appropriate technical and organisational measures in place to keep data secure; and that the processor's staff who will be engaged in processing personal data on behalf of PHP are subject to a duty of confidentiality and receive regular training in data protection matters.

PHP will regularly review the activities and processes of any processors it uses, to check that the processor is processing personal data in line with its internal processes; complying with relevant requirements under the Data Protection Legislation and its contractual commitments in respect of the personal data. PHP will ensure that its contract with each processor contains provisions concerning sub-contracting which meet the requirements of GDPR.

## Data subjects' rights':

Data subjects are entitled to access their personal data held by PHP on request (Article 15 GDPR). The response to a data subject access request will include certain information, such as: the purposes of the processing; the recipients (or categories of recipient) to whom the personal data have or will be disclosed; and individuals' rights to have their data corrected, deleted or to restrict the processing of their data.

Under the GDPR, the information will be provided to data subjects free of charge and within one month of the request.

**The right to be forgotten**

Data subjects have the right to request PHP erase all data held in respect of them in various circumstances (Article 17 GDPR). However, the right to be forgotten is not an absolute right, and PHP is only obliged to give effect to a request in a number of specific situations, the most relevant of which are likely to be:

1) Where the purpose for which the personal data were processed no longer applies; or

2) Where PHP's processing of the personal data is based on consent and the data subject withdraws his or her consent.

**The right to rectification**

Data subjects have the right to have incorrect personal data about them corrected without undue delay (Article 16 GDPR).

PHP will endeavour to ensure that any personal data it processes is up to date and correct. Where an error or inaccuracy is discovered, PHP will correct this as soon as possible.

**The right to data portability**

Data subjects have the right, in certain circumstances, to access their data in machine-readable format and, where technically possible, to have their data transferred directly from PHP to another data controller

(Article 20 GDPR). However, the circumstances in which the right to data portability arises are limited and, at present, seem unlikely to be relevant to PHP.

**The right to object**

Data subjects have the right in a number of specific circumstances, to object to having their personal data processed (Article 21 GDPR).

PHP will review this policy annually and may amend it from time to time as it sees fit.

For further information about this policy, and the PHP's data handling practices, please contact:

Helen Hartley

07789 465383

info@pilates-health.com

By completing a registration form and by participation in the activities of Pilates Health Physiotherapy, I give my consent and agree to my data being managed and processed in accordance with Pilates Health Physiotherapy data protection policy: