**Paleo Fitness LTD**

**DATA PROTECTION BREACH PROCEDURE**

**Purpose of this procedure**

This procedure supports PALEO FITNESS LTD’s Data Protection Policy and describes what a breach in data protection is and what process to follow in the event of one or more occurring.

**What is a Data Protection “Information” breach?**

The term information refers to information and data as defined within LABGC’s Data Protection Procedure. If information is lost, stolen or shared with others who are not authorised to receive or hear this, then an information breach has occurred.

**What steps to take in the event of an information breach.**

If you believe an information breach has occurred, you must complete the form **“Data Breach Reporting Form”** as soon as possible and within 24 hours and forward it by email to PALEO FITNESS LTD’s Data Controller : mark@Paleofitness.co.uk

The Data Controller will assess, using the information you have provided, whether a breach has occurred. They may contact you to help them make this decision. They may liaise with other colleagues to help them make this decision.

The Data Controller will let you know whether they believe an information breach has occurred. If they do not believe a breach has occurred, they will explain why and if they do believe one has occurred, they will let you know what they plan to do.

If a breach has occurred, there are four important elements to any breach management plan:

**1.** Containment and recovery

**2.** Assessment of ongoing risk

**3.** Notification of breach

**4.** Evaluation and response

Whilst this procedure details a range of steps and considerations, it is important to recognise that every situation will be different. The Data Controller will determine what is appropriate in each particular situation.

**1. Containment and recovery**

The Data Controller should lead this stage and take the following steps/consider the following aspects:

* Determine who needs to be informed of the breach. Ensure that only people who need to know or who will be involved in any investigation are informed.
* Agree a containment plan and ensure that everyone involved in the plan is clear what is expected of them and by when.

**Example:** If one of the servers has been compromised, we may decide to close down the server or part of it to ensure the issue is contained.

* Agree what else can be done to recover losses and/or limit any damage caused by the breach.

**Example:** In the event of a laptop being lost or stolen, we will identify what if any data is accessible by the laptop and take steps to ensure data loss is minimised by changing passwords for email and other systems accessed through the equipment.

**2. Assessing the risks**

Some information breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. An example might be where a laptop is irreparably damaged but its files were backed up and can be recovered, albeit at some cost to the business. While these types of incidents can still have significant consequences, the risks are very different from those posed by, for example, the theft of a customer database, the data on which may be used to commit identity fraud.

The Data Controller will assess the risk to PALEO FITNESS LTD, member and partner organisations of the information breach which has been reported to them. They will consider a range of things to inform this:

* What type of data is involved?
* How sensitive is it? Remember that some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details).
* If data has been lost or stolen, are there any protections in place such as encryption? What has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.
* Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.
* How many individuals’ personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment.
* Who are the individuals whose data has been breached? Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks. What harm can come to those individuals?
* Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
* Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service we provide?
* If individuals’ bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

**3. Notification of breaches**

By now, action should have been taken to contain the breach and an assessment of the risk to the organisation and individual undertaken. One of the most difficult steps is to determine who to tell. The key is to ensure that you know why you are telling someone what has happened and that your communication has a clear purpose. Sometimes it may be to ensure that individuals can take steps to protect themselves or to allow appropriate regulatory bodies to perform their functions. In some cases, we may need to report the breach to the Information Commissioner and/or the Charity Commission.

The Data Controller may want to liaise with member clubs, partners or colleagues, and in serious cases the PALEO FITNESS LTD board of trustees, in determining who to notify. The Data Controller will consider the following in determining who may need to be notified of this breach:

* Are there any legal or contractual requirements?
* Can notification help you meet your security obligations with regard to the seventh data protection principle? Can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act on the information you provide to mitigate risks, for example by cancelling a credit card or changing a password?
* If a large number of people are affected or there are very serious consequences, you should inform the ICO (see below for more detail to inform this).
* Have you considered the dangers of ‘over notifying’? You also need to consider who to notify, what you are going to tell them and how you are going to communicate the message.
* Are there any third parties who may need to be notified? E.g.: the police, insurers, professional bodies, bank or credit card companies who can assist in reducing the risk of financial loss to individuals, and trade unions.

**Notifying individuals**

If you have decided that an individual/s should be notified of a breach, the following points should be considered ahead of the communication:

* Give specific and clear advice on the steps they can take to protect themselves and also what you are willing to do to help them.
* Provide a way in which they can contact you for further information or to ask you questions about what has occurred.
* How will you communicate?
* Have you considered who the individuals are e.g.: are they vulnerable young people? What additional steps might you need to consider in these cases?

**Notifying the Information Commissioners Office (ICO)**

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals’ rights and freedoms, you must also inform those individuals without undue delay.

There is no legal obligation to notify the ICO of a data breach. However, PALEO FITNESS LTD have agreed that in the event of a serious breach, we will notify the ICO because we believe this is best practice.

The Data Controller must first determine if the breach which has been reported is a serious breach. Serious breaches are not defined by the ICO. The Data Controller will use the information they have collated on this matter and the risk assessment they have conducted and make recommendations.

The potential detriment to individuals is the overriding consideration in deciding whether a breach should be reported to the ICO. Detriment includes emotional distress as well as both physical and financial damage.

Ways in which detriment can occur include:

* Exposure to identity theft through the release of non-public identifiers, e.g.: passport number;
* Information about the private aspects of a person’s life becoming known to another, e.g.: financial circumstances.

Where there is significant, actual or potential detriment as a result of the breach, whether because of the volume of data, its sensitivity or a combination of the two, there should be a presumption to report.

Where there is little risk that individuals would suffer significant detriment, for example because a stolen laptop is properly encrypted or the information that is the subject of the breach is publicly available information, there is no need to report.

There should be a presumption to report where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. Each case must be considered on its own merit. However, it will be appropriate to report much lower volumes in some circumstances because of the loss or the extent of information about each individual.

**Notifying the Charity Commission**

The responsibility for reporting serious incidents within the Charity rests with the County Director guided by the Board of Trustees.

In the event that LABGC has deemed an information breach sufficiently serious to notify the ICO, then consideration must be given to also notifying the Charity Commission. The County Director will discuss the situation with the Board of Trustees and agree if a report needs to be submitted.

The Charity Commission’s “Reporting Serious Incidents – A Guide for Trustees” document should be referred to and the process defined by the Charity Commission followed.

**4. Evaluation and response**

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of our response to it. Clearly, if the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing ‘business as usual’ is not acceptable; similarly, if our response was hampered by inadequate policies or a lack of a clear allocation of responsibility, then we will endeavour to review and update these policies and lines of responsibility in the light of experience.