mypthub iCaaS

TOP 10 TIPS

FOR PERSONAL TRAINERS WORKING FROM HOME

Here are 10 ways Personal Trainers can protect their reputation and their brand

1 Effective training

With over 90% of cyber data breaches down to human error, Personal Trainers can reduce the risk of breaches with effective training. In turn this will avoid fines from the Information Commissioner's Office and the potential reputational damage that follows. Sending emails to the wrong recipients, downloading a malware-infected attachment or failing to use a strong password are all ways that human error could ultimately lead to a data breach. Many of these lapses in judgement happen due to lack of knowledge, because the employee is tired, distracted or not paying attention.

2 Classify data

Personal Trainers need to think about how classify their data – what is absolutely critical to their business, what needs to be protected from a regulatory perspective (such as the EU's General Data Protection Regulation), and what's actually not that sensitive. They then need to consider what has to be stored, and what doesn't.

3 Securing online video training sessions

All screensharing apps have vulnerabilities if not used correctly and the right security protocols are not adhered to. Video calls that are not secured by a password can be easily attacked by hackers. Personal Trainers must also ensure their teams only send meeting invitations with an associated password – especially if it contains sensitive information. This includes financial spreadsheets, HR files and CRM databases. This will also limit the risk of a data breach. The use of a strong password created by a random password generator will help to provide a link which cannot easily be hacked.

4 Using company equipment

Some Personal Trainers may have been loaned loaned computers and other devices to use while working remotely. Companies need to carefully consider potential risks and understand how these can be mitigated.

5 Secure home Wi-Fi

Home Wi-Fi networks are not likely to be as secure as a work network. Using a VPN will help to protect the connection, otherwise this could leave services exposed to hacking and allow unauthorised access to data.

6 Secure PC security software

Whether it is web security gateways, cloud security defences, encryption, or anti-malware applications, the reality is that significantly fewer of these are likely to be available at home or, if they are available, they could be poorly configured. The use of one-time codes sent to trusted phones or using a one-time PIN generation app, can help.

7 Protect personal devices

Being careless with mobile phone or laptop can lead to a data breach. Personal Trainers will most probably have a wealth of personal client data on these devices. Make sure they are not left lying around and are properly secured. Always lock the device if you are leaving it unattended.

8 Make sure security software is up to date

A firewall acts as a barrier, preventing unauthorised access to your device or network. This makes it harder for a hacker to gain access and helps to keep the information you hold on your device secure.

9 Use secure passwords

The device that you use, whether that be a company laptop or personal computer, must be protected by a strong password. Strong passwords are those that are a combination of at least 10 lower and uppercase letters, numbers and symbols. You must never use the same password for more than one account or write them down.

10 Keep hard copies of data safe

Not all data is kept online. When protecting sensitive data, you must also consider information which is in a physical form. Personal Trainers might still be handling letters or other hard copies, such as information you printed out or took home to use while working from home.

Research shows that 81% of clients would not use a Personal Trainer who had unlawfully disclosed personal information. Legal compliance is critical, but it is your reputation that is key when working as a Personal Trainer. The solution is easy to use and is supported by comprehensive online training.

TO LEARN MORE ABOUT DATA SECURITY & COMPLIANCE FOR PERSONAL TRAINERS, VISIT: HTTPS://MYICAAS.COM/MYPTHUB

iCaaS