



Hybrid Working

IT Hotdesk



[An overview...](#)

# How to achieve business success through hybrid working

An overview of how technology can support businesses, help staff improve productivity and plug any cyber security risks caused through anywhere working.

WELCOME

# Our guide to hybrid working

**For the majority of us, COVID-19 is the biggest global event of our lifetimes. And it's safe to say that in years to come, its impact will still influence our lives.**

It has challenged us, changed our behaviours and altered our perspective. A worldwide lockdown has forced us to slow down and re-evaluated what is important.

For many, flexible working has become the new normal and businesses rely on the ability to work anywhere - whether that's the office, their home or even a cafe.

Although restrictions are continuing to ease and while most businesses have started to phase their return to the office, the last 2 years have proven that people can, and want to, work at home as well as the office.

This whitepaper is a guideline for businesses, a look into the technology available and how it can be used to improve productivity and increase security.

As we take our next steps, it's important that we remember that it's not about getting "back" to normal; it's about creating a new one.

Managing director

Gordon Christie

# Table Of Contents

Overview	4
Have a robust infrastructure in place	5
Investing in the right technology...	6
Implement stricter security controls	7

### What is hybrid working?

Hybrid working is when staff split their time between their office and at home, or an alternative work location. Pre covid, it would have been that our customers spent 99% of their time in the office working and would only work from home occasionally.

## Overview

### Understanding anywhere working...

Essentially, hybrid and anywhere working are the same thing.

Hybrid working is traditionally split between the office and home, whereas 'anywhere working' is exactly as it sounds - working from anywhere. Whether that's at home, in the office, or even at a third party space like a coffee shop, hotel or conference centre.

The ethos of hybrid and anywhere working is the same - providing the tools and for flexible working, regardless of the location.

At the beginning of the pandemic, we viewed working from home as a temporary fix that would be phased out as the world opened back up again. Two years on, it's clear that anywhere working is very much here to stay so businesses need to adapt to support it.

There are three key fundamentals to successful anywhere working, infrastructure, technology and security, which I discuss in further detail throughout this article.

## INVESTMENT

# Have a robust infrastructure in place

To truly be successful at hybrid working, I believe that the focus needs to be on setting up the right infrastructure for your staff. Ideally, you want it so that your staff can work from anywhere - whether that's in the office, at home, or even in a coffee shop.

## 85%

of employees currently working from home want a 'hybrid' approach of both home and office working in future

When I say infrastructure, I don't just mean IT infrastructure, business owners and managers also need to look at the support required for remote work, such as flexible work hours, company meetings, time tracking and more.

There are four pillars that strengthen the success of hybrid working - culture, the people, processes and technology.

**Creating culture when people work from everywhere.**

The most important thing to realise about hybrid working is the intentionality and effort necessary to maintain culture. It won't come naturally, as culture has always been a challenge that businesses strive to strengthen and sustain, but with hybrid working, the strain will be significantly increased. Now more than ever, take the time to develop and embed your companies culture. It won't be easy, but the results will be worthwhile.

**Encourage regular communication.**

Working from home can feel isolating. And the best way to minimise this is for staff to stay in touch with each other, whether that's a morning check-in, instant messaging or video calls.

Encourage staff who work from home to stay active in the group chat. And at the office, where possible avoid emails and messenger apps. Get up and talk with people.

Staying connected helps employees feel part of a team which can help you to stay motivated, which helps maximise productivity.

**Update workplace processes to incorporate hybrid working.**

Incorporating hybrid working into the workplace requires the standard rules and boundaries being updated. Ensuring that all staff are aware of what the new rules are will help everyone understand what's expected of them and their colleagues.

**Establish what your team needs to thrive, regardless of where they are working.**

Hybrid working used to be the exception, not the rule but this is no longer the case, You need to provide staff with the tools required to allow for anywhere working. Whether that's travel sized equipment, additional screens and chargers, or adapting the systems in place, you have to weigh up the cost of loss of productivity, compared to the required spend for additional equipment.

Arguably, each element is equally as important as each other, today we will cover the technical aspects and how they can impact a business.

# Investing in the right technology...

**The right technology tools are a must for any remote-first infrastructure. All employees need to be able to easily communicate, collaborate, share ideas and stories the same as they would if they are working in the office.**

Technology should act as an enabler – helping organizations connect employees and customers, transforming hybrid working and streamlining the process.

There are several technologies that can support anywhere working, including:

## Cloud Solutions

Having all of your applications and data in the cloud means that you can work from anywhere with an internet connection - even on your commute to work. Cloud solutions also act as a backup solution, adding a level of business continuity.

## VPN

If you decide against a cloud solution, and store your data on an on-premises server then installing a VPN will be the best business decision you make today - or at least when it comes to your IT solutions! VPN will allow employees to securely connect to your work network so that it feels just like you are in the office.

## Remote Access Tools

One of the easiest options to include in your hybrid working strategy is remote access tools. Although it's easy to install, it's worth noting that it also poses one of the highest security risks. A lack of physical control may expose your business to eavesdropping - where information travels over the public internet.

## Understand what's essential to you...

Although it would be nice to have cloud storage and IP telephony, both technologies are not business-critical.

For me, I would say that the must-have technology for hybrid working is video conferencing, messaging tools and time tracking software, such as Free Agent.

# Implement stricter security controls

The upsurge in remote working has caused existing security threats to be amplified. In the office, employees are typically working behind layers of security controls. However, when employees leave the office and work from new locations, unique cyber security challenges arise.

Unmanaged mobile devices and insecure home wifis and networks increase the likelihood of a cybercriminal successfully infiltrating an IT system. There are a few steps that can be taken to improve your business security:

**1. Install updates** - Ensure that all devices have the latest firmware installed on them and are regularly updated.

**2. Encrypt your home Wi-Fi** - Encryption scrambles the information sent through your network, making it harder for other people to see what you're doing or recording your personal information.

**3. Change your router's preset passwords** - Some routers come with preset passwords out of the box which may seem handy but hackers can easily find these passwords, so it's important to change them to something more complex. There are two passwords on your router, the Wi-Fi network password and the router admin password, so make sure that you update both of us.

**4. Turn off remote management** - WPS lets you push a button on the router to connect a device to the internet instead of entering the network password. UPnP lets your devices find each other on the network. These features may make it easier to, say, add devices to your network or let guests use your Wi-Fi — but they can make your network less secure.

**5. Set up a guest network** - Many routers let you set up a guest network with a different name and password. It's a good security move for two reasons:

- Having a separate login means fewer people have your primary Wi-Fi network password
- In case a guest (unknowingly) has malware on their phone or tablet, it won't get onto your primary network and your devices.

**Unsure about your anywhere working strategy? Our team of IT experts are on hand to help. Book your free strategy review [here](#).**



**Our address:**

23 Abercrombie Court  
Aberdeen  
AB32 6FE

**E-mail:**

[info@ithotdesk.com](mailto:info@ithotdesk.com)  
[www.ithotdesk.com](http://www.ithotdesk.com)

**Phone:**

0800 640 3955