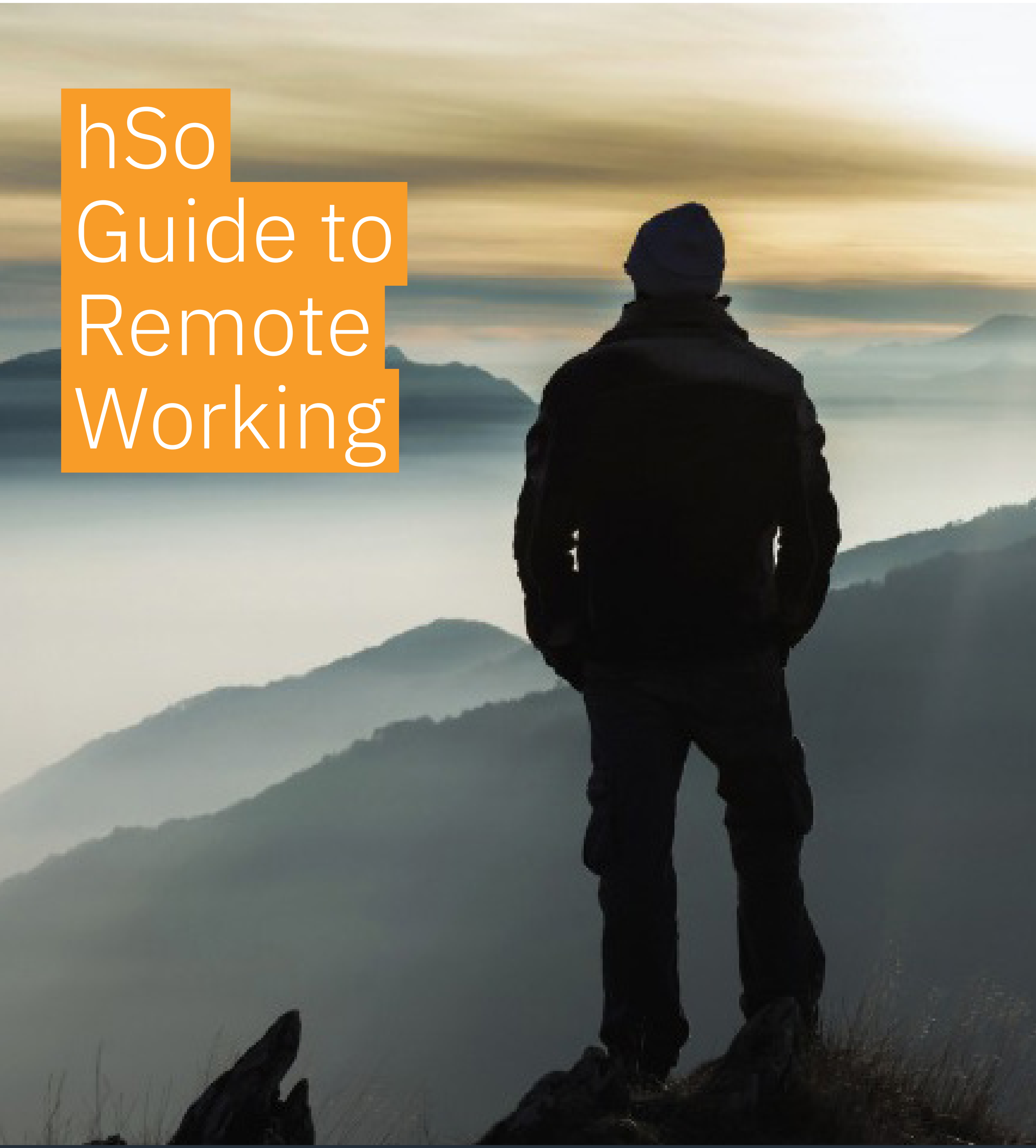
hSo:

CLOUD
NETWORK
SECURITY



hSo Guide to Remote Working

Legal Disclaimer

This free guide is designed to provide only general guidance on Remote Working.

Whilst HighSpeed Office Limited, trading as hSo (“hSo”) makes all reasonable endeavours to ensure the accuracy of the information in this guide, hSo accepts no liability to you or anyone else for any action taken in reliance on this guide.

The guide is not intended as a substitute for professional advice. Before making any decision or taking any action in reliance on the information contained in the guide, an appropriate professional advisor should be consulted.

Microsoft, Windows, Office, Active Directory are trademarks of Microsoft Corporation. Android is a trademark of Google LLC. Mac and macOS are trademarks of Apple Inc. IOS is a trademark of Cisco licensed to Apple Inc. in relation to iOS. Slack is a trademark of Slack Technologies, Inc.

Copyright Notice

00

CONTENTS

01

The Business Case for Remote Working in 2020

Reduce the Disruption Caused to Your Organisation by the COVID-19 Coronavirus Pandemic

The COVID-19 coronavirus pandemic is likely to adversely impact much of the UK population, including many of your organisation's employees. Employees that catch the virus will need to self-isolate to avoid infecting others. Infected employees will not be able to travel to work, even if their symptoms are mild and they feel well enough to work.

To help mitigate against the adverse impact this could have on your organisation and its customers, you need to have a good remote working solution in place – one that's secure, scalable and feature- rich. If you don't yet have such a solution, you need to fix that quickly. Luckily, sorting out remote working will stand you in good stead long after the threat of COVID-19 has receded.

Here is a reminder of the more usual reasons for deploying remote working:

1. Retain Staff
2. Fill Job Vacancies More Easily
3. Fulfil Your 'Flexible Working' Legal Obligation
4. Make Your Staff More Productive
5. Make Overtime More Convenient
6. Stop Your Staff Creating Their Own Ad-hoc Remote Working Solutions
7. Reduce Business Disruption Caused by Snow, Flooding, Rail Strikes and Roadworks
8. Cut Your Office Costs (In the Long Term)
9. Reduce the Impact of Sickness
10. Be Greener
11. Boost your Business Continuity Plan

1. Retain Staff

For some of your staff, there will come the point where they reconsider their future at your firm. They like their job and their coworkers but find their commute too long and costly.
Remote working can help you retain such staff without having to raise their compensation. Allowing staff to work from home isn't primarily about keeping staff happy. Staff turnover costs a fortune in recruitment agency fees, management time, business disruption and training costs. If your organisation can retain valuable employees for longer, at minimal cost, by offering remote working, that saves your organisation money and avoids unnecessary disruption.

2. Fill Job Vacancies More Easily

Most organisations have made a job offer to a potential employee, only to be turned down because the package on offer wasn't viewed as being sufficiently attractive. The ability to work from home occasionally is an inexpensive benefit that will make your job offers more appealing. Remote working also makes it possible for your organisation to recruit from a wider geographic area.

3. Fulfil Your 'Flexible Working' Legal Obligation

ALL UK employees that have been employed for 26 weeks are entitled to request flexible working. Remote working solutions help you accommodate these requests, with minimal business disruption. For example, by allowing staff to work from home a few days each week or letting them work flexible hours around the school run.

4. Make Your Staff More Productive

Surprisingly, studies show that far from slacking off, most remote workers put in *more* hours than they're supposed to. This may be because they are keen to get work finished and to show they really are working.
Those working remotely often face fewer distractions than their colleagues working in noisy open- plan offices.

5. Make Overtime More Convenient

Sometimes, overtime is unavoidable. Remote working allows staff to finish the job from home without having to stay late at the office or come in over the weekend.

6. Stop Your Staff Creating Their Own Ad-hoc Remote Working Solutions

If you don’t offer remote working solutions, remote working will still happen. It will just happen insecurely. Employees may email the files they need to their personal email account, copy them to unencrypted USB sticks, or install remote access software on their work computers without your knowledge.

Secure remote working solutions give staff access to the information they need without compromising data security.

7. Reduce Business Disruption Caused by Snow, Flooding, Rail Strikes and Roadworks

You can’t do anything to stop it snowing. But you can ensure your staff aren’t forced to waste hours fighting travel chaos to get into an office to do work that could have been done at home.

8. Cut Your Office Costs (In the Long Term)

Each empty desks costs your organisation thousands of pounds each year in rent, business rates and service charges. The unused space also adds to your insurance, lighting and heating costs. Remote working, when combined with hot-desking, can slash your office costs. When your office lease comes up for renewal, you can save a fortune by moving to smaller offices. Or you can consolidate unused space and sub-let it, subject to your landlord's approval. If your organisation has a growing workforce, remote working helps you put off the day when you are forced to move to a larger, more expensive office.

9. Reduce the Impact of Sickness

Sometimes staff are well enough to work, but not well enough to come into the office. For example, a sports injury might impede someone’s mobility, making commuting impractical. Or perhaps one of your staff has seasonal flu and you don’t want to risk them spreading it to colleagues. Sometimes your employees will need to be at home for reasons other than sickness, for example to receive a large delivery or to let the builders in.

If you don’t give your staff the tools to work from home on such occasions, they will be forced to take time off, often at short notice. That is far more disruptive than letting them work remotely occasionally.

10. Be Greener

Remote Working cuts commuting, reducing your organisation’s carbon footprint. If you truly embrace remote working and hot-desking, you can cut your office space requirements, reducing the amount of energy wasted on lighting, heating and air-conditioning empty desks.

11. Boost your Business Continuity Plan

Remote working helps you cope with adverse events that are likely to happen – such as travel chaos caused by poor weather conditions or strikes. It could also help you mitigate the impact of unlikely events with potentially catastrophic consequences e.g. office fires, floods and extended power outages.

02

How to Successfully Roll Out Remote Working

View the roll-out of remote working as a series of steps, some of which can be completed later when you have more time. You don’t need to roll out a perfect solution to everyone on day one.

01 **Start with a Small-Scale Trial**
Roll out remote working to your IT team first, so they are familiar with the technology and can quickly iron out any firewall-related problems and user-authentication issues. Extend the trial to senior staff, to generate organisational buy-in. Suggest users work from home for just one day a week initially, so everyone can slowly acclimatise to the new arrangement.

02 **Deploy a Virtual Private Network (VPN)**
This will protect the confidentiality of data flowing to and from your remote workers over untrusted networks. Ask remote workers to use remote desktop tools to connect to their work computers. Users will be able to access their emails and applications, but you won't need to buy additional software licenses or protect extra devices

03 **Add an Instant Messaging and Presence Tool**
This will give staff a fast and intuitive way to communicate with colleagues in other locations and show them who is available and at their computer. Presence works best when the software is integrated with employees' calendars, so the system can automatically show which members of staff are in a meeting, which have the day off etc.

04 **Add Telephony**
Ask remote workers to divert their office phones to their mobiles. In the longer term, consider deploying VoIP, so remote workers can call the office for free and answer calls to their office number from home. Some unified communication solutions combine instant messaging, presence, telephony, video conferencing and screen sharing in a single piece of software per OS, potentially speeding up your remote working roll-out.

05 **Roll Out the Trial to Progressively More Employees.**
Encourage Staff to Work Remotely More Often. The aim is to uncover unforeseen obstacles to wider adoption of remote working, so you can address these before widening the roll-out further.

06 **Sort Out The 'HR' Paperwork**
Create a remote working policy that explains who can request remote working, how they should do so, what behaviour is expected and what Health & Safety standards need to be met.
You may need to update your standard employment contract to reflect the new arrangements then ask existing employees to sign amended contracts.

07 **Provide Training To Staff (Including Special Training For Managers)**
Book some training sessions on Working Remotely and Managing Remote Workers.

08 **Introduce Additional Collaboration Tools**
Such as screen sharing software, video conferencing, online project management tools and wikis.

03

Technology That Can Help Make Remote Working A Reality

There are four key elements of remote working that you need to think about: connectivity, security, telephony and screen-based collaboration. These elements may involve a wide range of technologies, including the following:

Consumer Broadband

Most of your remote workers will be working from home, where they already have broadband, provided by a consumer ISP.
Relying on these existing connections has two major advantages – these connections already exist, and your organisation typically doesn't have to pay towards the broadband bill. You just run a VPN over the top and give your staff collaboration tools.

Business Broadband

Some organisations get their most frequent remote workers a second broadband connection just for business use. Unlike employees' own broadband connections, these employer-funded connections come with service level agreements, 24/7 support, shorter waiting times for technical support, higher- specification routers, less traffic throttling, and static IP addresses.
The organisation picks up the tab, so can liaise directly with the ISP rather than leave employees to sort out connectivity problems for themselves.
Troubleshooting is simplified, as there is a single ISP providing most of the connectivity underpinning the remote worker apps. Most employees will have routers from the same vendor, often the same model of router, and they are subject to the same ISP traffic-management policies, which helps make network performance more predictable, and technical trials more representative of what will happen when you roll out applications more widely.
Business broadband doesn't have to connect directly to the Internet. Some ISPs can connect broadband lines to your office network or WAN instead, if that is preferred. This option may eliminate the need for a VPN. It also makes it possible for Unified Threat Management device(s) to protect and manage the Internet use of employees in the office and at home.

Public Wi-Fi and Mobile Broadband

Some staff may need to connect to your network when travelling on business. Your remote working strategy needs to accommodate such staff connecting via public Wi-Fi or mobile broadband.

When using public Wi-Fi, a VPN should be used to stop other network users and rogue Wi-Fi hotspot operators from snooping on your organisation's traffic.

If you just want to connect remote workers' company-issued laptops to your network, one option is to provide a mobile connection that connects directly to your office network or WAN, instead of sending data over the Internet. This may do away with the need for a VPN.

Leased Line

If dozens (or hundreds) of staff remotely connect to desktops or servers in your office that increases the traffic flowing to and from your office. Check you have enough bandwidth for this. You may have enough. If not, you don't necessarily need to upgrade your leased line. Moving some servers/devices from your office to colocation space may help and is likely to be quicker to implement.

VPNs

These use encryption, authentication and data integrity checks to create secure tunnels through insecure public networks such as the Internet.

SSL VPNs let your staff connect to your network via a standard web browser. They use the same port numbers and protocols as typical web sites, so seldom run into problems traversing firewalls. This makes SSL VPNs ideal for remote working, especially where remote workers are connecting from their own computers/tablets. Optional OS-specific software may be available to add features such as automated connection to the network on start-up, split tunnelling, and improved endpoint security.

IPsec VPNs are your other main option. They are popular with organisations that issue corporate- owned corporate-managed computers/tablets to staff. The IT team has full authority over the devices and installs VPN client software and any certificates required for authentication.

Whichever VPN type(s) you select, try to find something that integrates with your organisation's existing identity-management solution e.g. Microsoft Active Directory, so users can log on with their existing credentials, and when accounts are disabled/deleted, VPN access is cut off automatically.

Unified Threat Management

This helps protect your users and your network from attacks and from inappropriate network use. Next generation firewalls combine deep-packet inspection and nuanced rules to block, filter and rate-shape traffic in a manner that's application-aware, content-aware and attack-signature-aware.

More prosaically, UTM blocks misguided remote workers from downloading malware and accessing inappropriate content. UTM stops your VPN becoming a backdoor into your corporate network for application traffic you don't wish to allow to run over your network. This is particularly relevant if remote users are connecting to your network from personal devices over which you have no control.

Unified Communication (UC)

This bundles useful collaboration features into a single integrated piece of software. We recommend that UC forms a key part of your remote working toolkit.

Here are some of the features UC software may offer:

Instant Messaging – Text-based chatting. Two or more individuals can communicate with each other in real-time or asynchronously. More immediate than email. Less interruptive than a phone call.

Software-based VoIP – Telephony, without having to pay for physical handset. The software may support click-to-call, and typically when users receive a call from a known contact the details for that person will pop up on screen. VoIP usually allows remote workers to answer their work number from wherever they are and to make calls from their work number without being personally billed.

Voicemail – Leave a message after the tone. Less obviously, alert users to their new messages, show the name of the person who left the message (if known), allow messages to be played, deleted, saved or forwarded. Allow voicemail greetings to be re-recorded.

Audio Conferencing – Calls with more than just two people on the line. A helpful alternative to getting everyone in the same physical meeting room, which isn't always feasible.

Presence – Shows whether colleagues are in meetings, on the phone, on leave, away from their desks, or not to be disturbed. Presence tools may allow managers to see at a glance which members of staff appear to be inactive or away from their device.

Screen Sharing Tools – Several people can view the same computer screen at once. One person might use it to go through a PowerPoint presentation, another might show work in progress, a third person might load a web site to clarify a point under discussion. Combine this with audio conferencing for a powerful alternative to routine face-to-face meetings.

Desktop Sharing Tools – Screen sharing, but with the ability of participants to grant others the ability to non-exclusively control their mouse and keyword.

Video Conferencing – This used to require expensive conference suites. Not any more. Now, most workers have webcams built into their laptops/tablets/Macs or can add USB webcams to their desktop PCs cheaply.

File Sharing – Specifically, sharing files securely with members of a particular workgroup or followers of a particular chat channel.

UC software is usually available as a collection of OS-specific applications, one for each major operating system. So these features tend to be available on mobile phones and tablets, not just on laptops and desktops.

Online Project Management Tools

These help teams – including teams that are geographically separated - collaborate on complex projects with countless tasks and interdependencies, where it can be difficult to keep track of things.

The work of each project team is broken down into tasks which can be assigned to individuals. Deadlines can be set, dependencies documented, and rates of progress can be analysed.

Some of these tools provide a shared space for documents and support threaded discussions. Managers can see which bits of work have been completed, and which employees already have more than enough tasks to keep them busy.

Popular project management tools include Basecamp, Asana, Wrike and Monday. Some organisations prefer to use drag-and-drop Kanban boards that list tasks to be done, tasks in progress, and tasks completed. In such cases, Jira, Trello or Microsoft Planner may suffice.

Web-Based Alternatives to Desktop Applications

Just because your staff use desktop applications when in the office doesn't mean they necessarily need to use those same desktop applications when working remotely.

In some cases, there may be web-based alternatives that would make everyone's life easier.

For example, if your organisation subscribes to Office 365 / Microsoft 365, and uses the hosted email, your users may be able to log on to a web-based version of Outlook by visiting www.office.com .

Microsoft offer web-based versions of Outlook, Teams, SharePoint, and several other Office apps.

Physical VoIP Phones and Landlines

Sometimes, a senior member of staff who works from home may ask for a physical office phone.

There are two ways to accommodate such requests: give that person a VoIP handset or give them a standard phone on a second landline, billed to the company.

VoIP handsets – like the ones in your office – aren't cheap and they aren't essentially portable. That is why you should try to encourage staff to embrace software-based VoIP, rather than request physical handsets. Despite the initial hardware costs, these phones save money, as calls made via them are significantly cheaper than if the same calls had been made via an ordinary landline or mobile. What's more, there's no line rental to pay. You just pay for the phone number (DDI) instead. If the employee leaves, you can redirect their number to another employee.

Your second option is to give your employee a new landline – paid for by your organisation. Your organisation pays line rental and call charges that are higher than if you had used VoIP. The primary benefit is that this provides an easy way to allow employees to make business calls without incurring personal expenses which then have to be claimed back. It's your organisation's landline, so you get an itemised bill, allowing you to keep an eye on how the line is used.

Microsoft Teams

If you are evaluating collaboration tools to underpin your remote working strategy, Microsoft Teams should be on your radar. Teams is Microsoft's flagship real-time business communications product and is used by over 44 million users. Teams is unified communications software that offers:

- Instant messaging in channels
- Presence information
- Audio conferencing
- Video conferencing
- Screen sharing
- File sharing
- Inline file viewing (Excel, Word etc)
- Task management (from early 2020)
- Telephony (requires Microsoft Calling Plans or Microsoft Direct Routing)
- Native applications for Windows, macOS, Android, iOS and Linux. Plus a web app.

If your organisation subscribes to Office 365 or Microsoft 365 you may already be paying for Teams.

The paid version of Teams supports scheduled meetings and comes with administration tools, usage reporting and a service level agreement. There's also a free version that has fewer features, lower file size limits and a limit of 300 users per organisation. The free version is feature-rich and often sufficient for evaluation purposes.

If you already have the paid version, the free version may still be of use as it lets your suppliers use Teams to communicate with you, even if they don't have a relevant Microsoft subscription.

Microsoft is gently nudging over 200 milllion users of Office 365 to try Teams. Generous product bundling and integrations with products like Outlook have helped Teams become more popular than arch-rival Slack.

Typically, Teams users can call one another for free using Teams. However, as not everyone uses Teams, Microsoft has added several ways for users to make and receive standard phone calls via Teams.

One option is to buy call bundles from Microsoft known as Microsoft Calling Plans. These are then assigned to individual users.

A better option is to use Microsoft Direct Routing. This creates a connection between Microsoft and your phone company, allowing staff to make and receive calls on their existing work phone numbers via Teams.

Microsoft Direct Routing is usually significantly cheaper than Microsoft Calling Plans, as most employees don't make enough calls each month to justify paying for large call bundles. However, not all phone companies support Microsoft Direct Routing.

Phone companies that do support it usually offer the option of physical handsets, so your staff can have the best of both worlds - convenient software-based VoIP on their laptops, mobiles and home-based desktop computers, plus the option of keeping a physical phone - usually one that sits on their desk in the office.

04

Remote Working and The Law

Health & Safety Rules Apply to Remote Workers

Your organisation is responsible for the Health & Safety of all its employees, including those working remotely.

Make sure your remote workers are aware of good Health & Safety practices. Get them to confirm in writing that they will ensure their remote working environment complies with such requirements.

Employment Contracts May Need to Be Amended

It's not uncommon for contracts to specify that the employee is to work at a specific address – typically a designated office. You may need to amend your employment contracts to cover the fact that some employees may be allowed to work remotely, at least part of the time, subject to their line manager's discretion.

Check Insurance Contracts

Check whether your corporate insurance policies cover employees working remotely.

Data Protection

You need to take appropriate measures to protect personal data and commercially sensitive data. This is largely a matter of following standard IT security best practices, training staff on these practices, and ensuring that remote workers have a shredder to help dispose of sensitive printouts.

05

Flexible Working

All employees in the UK are entitled to request flexible working arrangements, once they've worked for their employer for at least 26 weeks.

Organisations don't have to approve such requests but must consider them in a 'reasonable manner.'

Flexible working can take many forms. These include:

- Working from home
- Flexi-time (Discretion over when work is done. May include fixed 'core hours' of work)
- Part-time working
- Job-sharing
- Compressed working hours (e.g. working four 10-hour days instead of five 8-hour days) Remote

working solutions help you deliver the first two of these, ***working from home*** and ***flexi-time***.

Employers can reject an application for any of the following reasons:

- extra costs that will damage the business
- the work cannot be reorganised among other staff
- people cannot be recruited to do the work
- flexible working will affect quality and performance
- the business won't be able to meet customer demand
- there's a lack of work to do during the proposed working times
- the business is planning changes to the workforce

Source: www.gov.uk/flexible-working/after-the-application

06

Adapting Your Remote Working Strategy to Reduce Coronavirus Disruption

A faster-than-usual roll-out of remote working is advisable

If you don't already have a good remote working solution in place – offering VoIP, instant messaging, presence and screen sharing – fix that now, so your organisation is better prepared for the first wave of the coronavirus pandemic, or failing that, subsequent waves that may occur later in the year.

Ordinarily, it is smart to roll out remote working gradually, giving IT staff a chance to familiarise themselves with the solutions, letting senior managers have early access to generate organisational buy-in and having trialists uncover technical niggles before other users encounter them.

The COVID-19 pandemic means you may have to deploy remote working more quickly than normal. A staggered roll-out of remote working is still sensible. You may just need to speed up the stages.

Be ready to offer remote working to far more employees and to support greater simultaneous use

Typically, organisations roll out remote working selectively. Not everyone is allowed to work remotely, and most employees that are authorised to do so may only do so a few days each week.

The COVID-19 pandemic has caused many organisations to reluctantly agree to greatly widen their use of remote working, so staff can still work while self-isolating with mild symptoms, and staff without symptoms can avoid catching the virus at the office or on their daily commute. However, a massive increase in remote working does have technical implications.

If many employees will be using Remote Desktop Protocol at the same time to access resources hosted at your office, you should consider whether your office Internet connection is fast enough to cope with the extra traffic. If not, one option is to upgrade the connection. A quicker option may be to move some of your devices and virtual machines from your office to colocation space or cloud- hosting, to divert some remote-worker traffic away from any leased line bottleneck.

Roll out modern collaboration tools to provide a digital alternative to some in-person meetings

In normal times, staff that work remotely still come into the office for meetings, so you can get away with deploying a basic remote working solution that only covers email, calendars and VPN access, with staff diverting calls to their mobiles.

If in-person meetings become less practical, you need to provide staff with a suitable digital substitute for such meetings, as postponing these meetings for months isn't really a viable option.

In practice this means you will need to give staff tools that let them conduct ad-hoc conference calls, screen-sharing/desktop-sharing and possibly even low-end video conferencing. To put it another way, unified communication has gone from being a nice-to-have to being an essential tool.

07 Remote Working Services From hSo

hSo can provide the key elements you need to successfully roll out remote working.

Connectivity – We provide business broadband connections, connecting these to the Internet, offices or WANs. We can connect your offices with leased lines that deliver the bandwidth necessary to handle simultaneous connections from hundreds or thousands of remote workers.

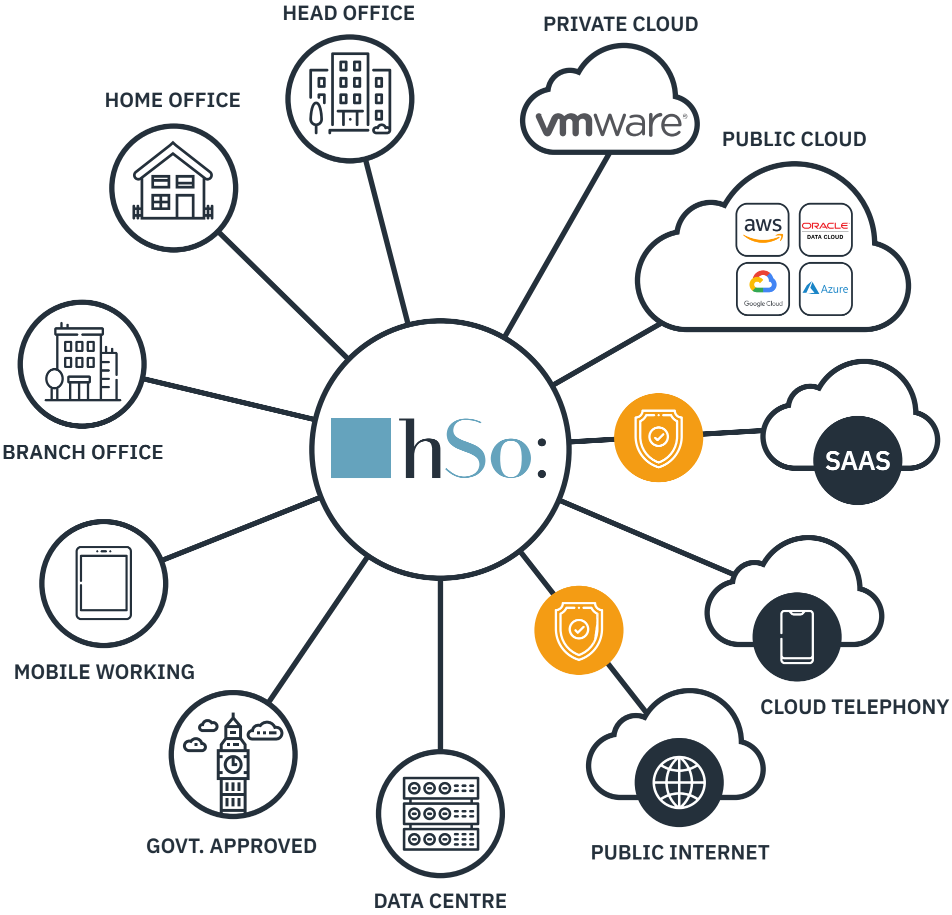
Encryption & Authentication – We offer both SSL VPNs and IPsec VPNs to protect your confidential data and can integrate these with Active Directory.

Network Protection – We can deploy Unified Threat Management (UTM) tools that help protect your users and your network from attack and from inappropriate network use.

Telephony – We offer business-class VoIP for remote workers that can integrate with office phone systems and with Microsoft Teams via Microsoft Direct Routing. We also provide standard landlines.

Collaboration Tools – We offer several unified communications options that help workers collaborate with features such as instant messaging, audio conferencing, video conferencing, and screen sharing.

All these hSo services are backed by Service Level Agreements and are supported 24x7 by our UK Customer Support Centre.



Your Cloud & IT Infrastructure Service Partner

- We understand your needs and offer guidance to selecting appropriate cloud solutions
- Enterprise-class data centres ensuring a high-standard of service consistency, technical support and application uptime
- Fully managed service from deployment, advanced monitoring, migration support to disaster recovery
- Expertise in advanced data and communication technologies and thought-leader in innovative solutions
- Service Level Agreements with your needs in mind and emphasising our level of commitment to you
- London-based team of technical experts on-call 24/7/365 to support you – anytime, anywhere
- Trusted by leading UK organisations

Discover hSo:

✉ info@hso.co.uk
☎ 020 7847 4510

www.hSo.co.uk

twitter.com/hSo
linkedIn.com/hSo-uk

50 Leman Street,
London, E1 8HQ

hSo:

CLOUD
NETWORK
SECURITY