FortressAS

YOUR CRITICAL HOME-WORKING QUESTIONS ANSWERED.

■ INTRODUCTION

When the COVID-19 pandemic hit, every company had to make a Digital Transformation almost literally overnight. Now, our production offices are in every employee home and we have found that it actually works well for the company, and for most employees.

However, according to the "Homeworker Wellbeing Survey" carried out by the Institute of Employment Studies in April 2020, just two weeks into lockdown, the cracks were already showing. Various physical health problems were being reported, with nearly 60% of respondents reporting neck pains/aches and leg pains.

With more people working from home, employers are seeking answers to critical questions to ensure they are adhering to legislation. This guide "The Definitive Home Working FAQ: Your Critical Home-Working Questions Answered" covers the answers to some of the most pressing questions employers have today about their employee's homeworking arrangements.

WHAT ARE THE REGULATIONS AND RISKS ASSOCIATED WITH PEOPLE WORKING FROM HOME?

Whenever your Employees work from home, whether it is from a dedicated office space, a desk in the corner of the lounge or a spot at the dining room table, they are classified as a home worker.

Typically, they will be carrying out their work activities in isolation from other people and without direct supervision.

Despite working remotely, Employers still have a duty of care to uphold; therefore, normal office health and safety requirements equally apply to Employees working from home.

WHO IS RESPONSIBLE FOR ENSURING HOME WORKERS HAVE A SAFE HOME OFFICE SET UP?

According to the Health and Safety at Work Act 1974, an Employer is responsible for an Employee's health, safety and welfare so far as is reasonably practicable.

In addition, the Management of Health and Safety at Work Regulations 1999 require Employers to undertake a general risk assessment. Businesses with five or more Employees must record significant findings.
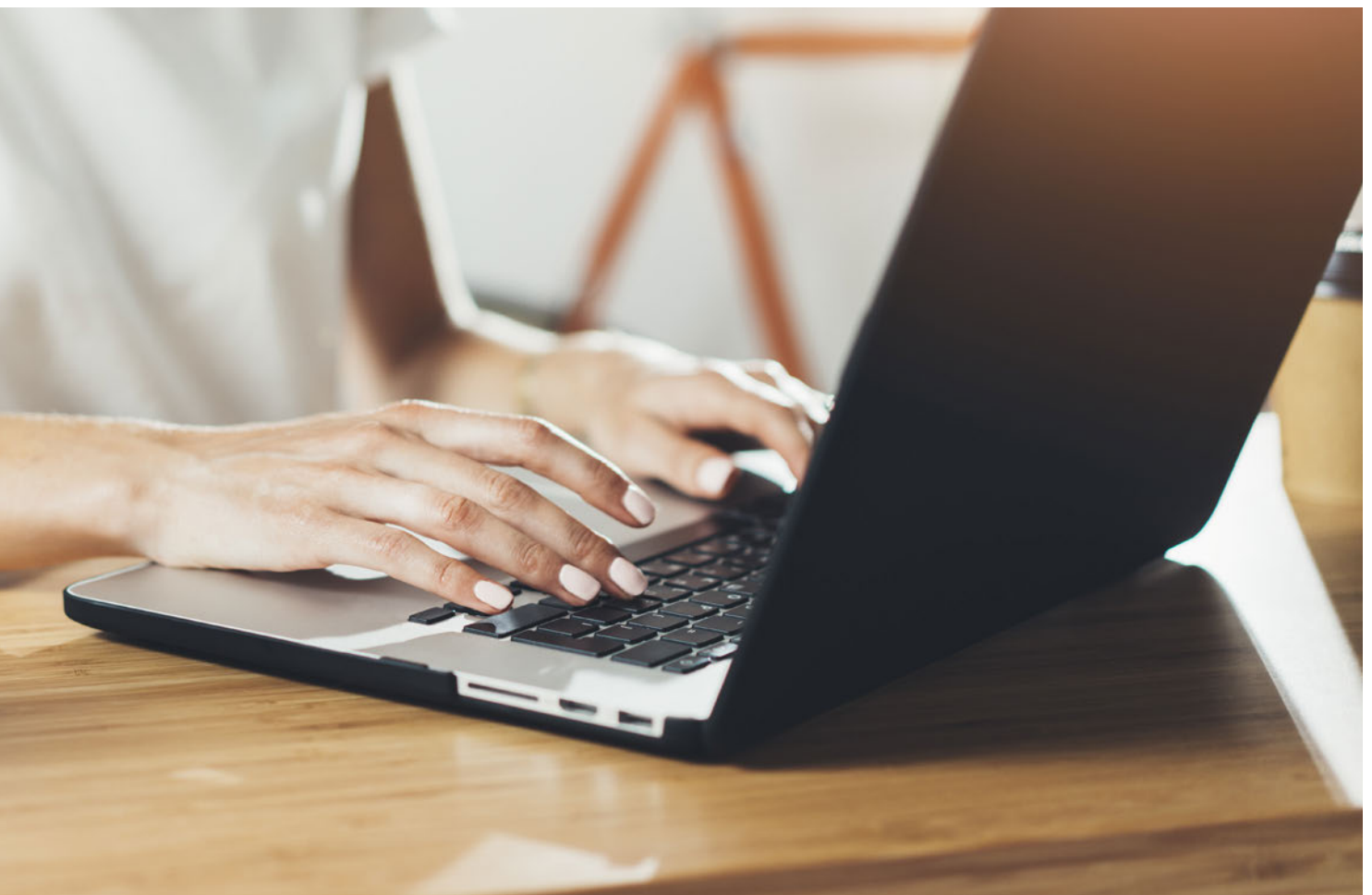
WHAT NEEDS TO BE REVIEWED AS PART OF A HOME WORKING ASSESSMENT?

Although most home workers will be completing low-risk, desk-based jobs, appropriate risk assessments still need to be conducted. This needs to be done at the start of the home working arrangement and periodically thereafter.

Employers need to assess the risks in the proposed home working space, including:

- Desk/work area
- Equipment
- Stress and welfare
- Slips, trips and falls
- Lone working

DESK/WORK AREA

There is a fine line between taking reasonable precautions and invading personal privacy. However, Employers need to assess the risks relating to the home working space.

Firstly, there needs to be enough free space – typically this is 11m³ per person – for the Employee to work comfortably. This work area needs to be clean, warm, well-lit and well-ventilated. There also needs to be enough room for the workstation and other equipment (e.g. printer). Normally, attics and cellars are undesirable home working environments because they tend to have limited access, a lack of natural light and poor temperature or ventilation control.

Regarding the workstation itself, there needs to be enough space for the Employee to stretch their legs and an adequate amount of surface space. It is their responsibility to keep the working area free of clutter to reduce any additional risks such as trips and falls.

EQUIPMENT

There is no legal obligation for an Employer to provide the necessary equipment for remote working. However, most companies find it easier to supply basic equipment – for example, a laptop – to ensure compatibility as well as maintaining data protection and security.

Access to a secure virtual private network (VPN) can allow Employees to connect to the company network from home. This provides access to relevant files and systems on the company network and to resources on the company intranet.

Portable electrical items require regular inspection to check that they are still safe to use. IT equipment often only requires a visual inspection by a competent person. After suitable training. this could be completed by the home worker themselves.

As in any office, a remote worker's display screen equipment (DSE) should be adjustable, clean and positioned to remove glare from a window or light. In addition, they should have an adjustable chair that has been ergonomically designed to reduce the risk of musculoskeletal problems.

STRESS AND WELFARE

Remote working hazards extend beyond the physical work environment. Home workers need to manage themselves in terms of taking regular breaks away from their workstation and carrying out stretches regularly to avoid stiff or sore muscles.

Employees that work from home may find it hard to manage their time or separate their work life from home life. For some, it can be difficult to turn off the computer and they may be tempted to work longer than normal hours due to the lack of supervision.

Simple things like installing a dedicated phone line for work that switches to an answer phone at the end of the day can help. Managers and team leaders should also monitor the times that home workers are sending emails. It may be appropriate to negotiate a 'lifestyle contract'.
Slips, Trips and Falls
According to the latest HSE figures, slips, trips and falls remain the biggest cause of workplace fatalities, responsible for 40 out of 147 reported deaths at work. Furthermore, slips, trips and falls on the same level resulted in 29% of non-fatal accidents in 2018/19.

To minimise these risks, remote workers need to ensure good standards of housekeeping in their workplace by removing trailing leads (from laptop, phone and other electrical equipment); keeping floor coverings (e.g. carpets and rugs) secure and clearing the area around their desk of boxes and papers.

LONE WORKING

In terms of lone working, working from home might not seem to present any immediate risks. However, what happens if the home worker suddenly becomes ill or is not visible online when they should be? The Employer needs to put a system in place where remote working Employees have to 'check-in' regularly. The member of staff working from home should also have the name and number of a supervisor who can be contacted easily.

Regular home workers have identified feelings of isolation from their organisation due to a lack of updates and not being informed about changes. Experiencing equipment issues that do not get fixed quickly also leads to feelings of frustration.

It is the Employer's responsibility to keep all their staff informed of organisational changes and any positions that become available so that remote workers do not feel professionally isolated. To combat this, the business could send out a daily or weekly update, letting staff know about company news, campaigns, events and details of any staff who have left.

Employers should also make provisions to support home workers that need technical assistance. A dedicated IT helpline could be set up so that staff working from home have remote access to IT support to solve any issues.

HOW DO I VALIDATE AND REGISTER THAT A HOME OFFICE SET UP IS SAFE?

Whilst the Employer is ultimately responsible for the safety and well-being of their Employees, wherever they are working, the validation process involves the Employer and the Employee.

EMPLOYER RESPONSIBILITIES

An Employer should be checking that:

- Each Employee feels the work they are being asked to do at home can be done safely
- Employees have the right equipment to work safely
- Managers are keeping in regular contact with their Employees, including making sure they do not feel isolated
- Reasonable adjustments are made for an Employee who has a disability

If changes are needed, Employers are responsible for making sure they happen.

EMPLOYEE RESPONSIBILITIES

Employees also have a responsibility to take reasonable care of their own health and safety.

Anyone working from home should keep in regular contact with their manager. They should also tell their manager about:

- Any health and safety risks
- Any homeworking arrangements that need to change

Therefore, while the workplace assessment process can be used to highlight potential hazards that the Employer will need to address, it is equally the responsibility of the Employee to make their Employer aware of any new concerns, or changes to their environment and well-being as soon as they occur. The Employer should then act responsibly and on a best-endeavours basis to help resolve the issues. Employers who fail to take reasonable steps could end up falling foul of their legal responsibilities.

CAN HOME WORKERS USE THEIR COMPANY DEVICE FOR PERSONAL USE IN THE EVENING?

A whole host of problems can arise when Employees use business equipment for personal purposes. Loss of productivity and the misuse of business resources can be curtailed with workplace policies that address the personal usage of business equipment.

Every business involves the use of some sort of equipment which Employees need to do their job, and this equipment is generally provided by the business. While some personal use of business equipment is realistically to be expected, problems can arise when the personal use is excessive.

Problems that can arise in the personal use of equipment that belongs to the business, such as computers, include:

- Broken equipment, which may cause disputes over who is responsible for repair
- Lost productivity, as Employees use work time for personal tasks involving business equipment
- Premature wear and maintenance on the equipment
- Morale problems if certain personal use habits are suddenly curtailed or if only some Employees can use the equipment

No matter what your policy is or how much you try to control it, Employees will probably use your equipment from time to time for personal purposes. The best way to handle the inevitable is to allow a reasonable amount of slack, but to be consistent and vigilant in creating and enforcing rules to make sure that the personal use does not get excessive.

Personal use of equipment that does not interfere with work is one thing, but how do you handle situations where the Employee plays games on the computer (or does some other kind of personal business) during work time? Your equipment and your Employees' habits will guide your handling of personal use situations. Be sure that whatever use you allow or prohibit is clearly communicated to all Employees and is consistently enforced.

CREATING A POLICY FOR THE PERSONAL USE OF BUSINESS EQUIPMENT

Your policy regarding the personal use of business computers could state that:

- Email and other computer files provided by the company are to be used for business purposes only.
- Use of computer facilities for personal reasons is strictly prohibited (alternatively, personal use may be permitted subject to approval).

The key is to create a policy that allows you to determine acceptable use and to apply that policy fairly and consistently.

- All computer passwords and codes must always be available to the company.
- No Employee may add unauthorised or pirated software or files to any machine owned by the business.

WARNING

If one of your Employees buys a great piece of scheduling software for use at home and installs it on your business's computer, you may be breaking the law. Software has strict copyrights, and "pirating" software is tantamount to stealing and the company is liable. If you need the software, you need to buy it and install it.

- Employees may not use computer files or software brought from home or other sources on the business computer (to avoid viruses).
- The company reserves the right to enter, search, and monitor the computer files or email of any Employee, without advance notice, for business purposes such as investigating theft, disclosure of confidential business or proprietary information, or personal abuse of the system, or monitoring work flow or productivity.
- Software or other business information on the computer should not be copied and taken from the business premises without permission.

Some companies also place the policy on log-in screens to appear each time the computer is turned on, to dissuade Employees from personal use of the equipment.

IN BYOD SCENARIOS, WHO IS RESPONSIBLE FOR THE SAFE KEEPING OF COMPANY DATA?

Employers are responsible for protecting company data stored on personal devices.

They should therefore consider implementing security measures to prevent unauthorised or unlawful access to the organisation's systems or company data, for example:

- Requiring the use of a strong password to secure the device.
- Using encryption to store data on the device securely.
- Ensuring that access to the device is locked or data automatically deleted if an incorrect password is inputted too many times.

Employers should ensure that its Employees understand what type of data can be stored on a personal device and which type of data cannot.

WHAT ARE THE TAX IMPLICATIONS ASSOCIATED WITH PEOPLE WORKING FROM HOME WITH COMPANY-OWNED EQUIPMENT OR BYOD EQUIPMENT?

If these are mainly used for business purposes and not significant private use, these are non-taxable, the same is true for BYOD devices.

SHOULD WE BE CONTRIBUTING TOWARDS THE BROADBAND COSTS OF HOME WORKERS?

If your Employee already pays for broadband, then no additional expenses can be claimed.

If a broadband internet connection is needed to work from home and one was not already available, then the broadband fee can be reimbursed by you and is non-taxable. In this case, the broadband is provided for business and any private use must be limited.

CAN WE INSIST THAT HOME WORKERS HAVE PROFESSIONAL BACKGROUNDS WHEN ON TEAMS/ZOOM CALLS?

This is entirely at the Employers discretion and must take into account how practical this is for their Employees.

However, with Microsoft Teams and Zoom both now featuring functionality that allows Employees to blur their backgrounds or replace their backgrounds with imagery, it is a lot easier for Employers to insist such features are turned on, assuming of course the Employee has the required equipment to enable the functionality to work.

For Employers to insist on the use of such functionality, they simply need to update their IT policy and procedures document and communicate the change to their impact Employees. It then becomes enforceable in line with every other documented policy.

WHO SHOULD THE HOME WORKERS CALL IF THEIR EQUIPMENT GOES WRONG?

This is entirely dependent on how the Employer wants the support to work.

The Employer may ask home workers to log all support calls with their internal helpdesk, in the same way they would for any other problem. In some cases, and due of the type of support home workers need, they may ask them to contact a third-party provider who is more geared up to ship replacement equipment and attend engineering calls at private addresses. In recent months, the latter is proving more common as internal helpdesk teams simply do not have the capacity to support such high quantities of home workers.

TALK TO US ABOUT OUR FortressAS HOME SERVICE

The FortressAS Home Service provides a single end-to-end solution delivering the assessment, improvement/supply and reporting needs that enable Compliance, HR, Facilities and IT to support home workers, thereby reducing risk to staff and to their companies. It delivers on a single SLA that a COO can refer to and report against.

Our Home Service simplifies the complexity of supporting home workers with regard to health and safety, technology and security. To find out more about the service and how we can help, visit https://fortressas.com/fortressas-home-service/ or contact us today.

ABOUT FortressAS
AVAILABILITY SERVICES

Fortress Availability Services Limited (FortressAS), CIR Specialist Provider of the Year 2019, was formed specifically to answer the Cyber and Operational Risk and Resilience needs of modern businesses.

With a focus on supporting the Financial Services Industry, FortressAS has built the most advanced work area recovery facility in the UK. The innovative and flexible resiliency and recovery services, supporting many banks, asset managers and insurers have this centre as their foundation.

Customer satisfaction is the driving force behind the FortressAS team's work, and they the winning entry to CIR Specialist Provider of the Year 2019 was a result of Customer commendations.

CONTACT US

Fortress Availability Services Limited
City Reach, 5 Greenwich View, London, E14 9NN

+44(0)20 3858 0099   info@fortressas.com