

We are here to help you.

Managing additional home working exposure



The spread of Coronavirus (Covid-19) is unprecedented and we understand this is an incredibly difficult time for families and businesses. We are here to help customers and businesses who are affected by the impact of Covid-19 in these challenging times and have created a guide on some of the risk measures to consider when working from home.

With the ongoing situation, many employers have asked their staff to work at home for an uncertain period of time. For many this will be their first experience of it. While the benefits of remote working go beyond limiting exposure to the Coronavirus, having potentially many more workers logging on to networks remotely and, in some cases, hastily setting up home offices, heightens other risks related to cyber security and personal safety. This change in working practices brings with it a range of new challenges and we highlight some of these below. Some of the recommendations made reflect best practice and may be difficult to implement in the present circumstances.

Health and Safety

Employers have established legal duties with regards to the safety, health and welfare of their staff that continue to apply with home working. Among other considerations, they need to make sure that the work activity and the temporary workspace are suitable and that appropriate equipment is provided.

Many employers have instructed all staff to work at home. However, in businesses such as supermarkets or schools providing for the children of key workers, this is not a viable option. If only a proportion of the workforce is to be asked to work from home, then the selection needs great care. Exposing somebody in their twenties to potential

infection may not present the same risk as for someone whose age or existing health condition makes them more vulnerable. You should have a document that illustrates your decision-making process.

Equipment that employees use in the workplace, such as a laptop, mouse, screen and keyboard can also be used at home. Any equipment does need to be suitable and in good condition. Turning to the home-working area, there needs to be adequate space that is safely accessed, with sufficient lighting and ventilation as far as possible. Electrical sockets, plugs and wires need to be in good condition and regular visual defect checks are recommended (staff should be given guidance on this). Also consider guidance on ensuring that only the recommended charging units are used for smart phones and tablets as the wrong combination can lead to overheating and present a fire risk. Ideally, any work area should have a smoke detector installed (with a working battery) and a fire extinguisher available. A good quality surge protector is recommended. In addition, leads should be managed to avoid presenting a tripping hazard.

Adequate guidance in respect of display screen equipment (workstation layout, breaks from DSE work, etc.) should be provided, as would be the case on the normal premises (see [Health and Safety Executive \(HSE\) website](#)). Best practice would be to ask employees to carry out a risk assessment (preferably with photographs) that can be checked centrally. However, the HSE emphasised on 18th March that “if you have people working from home temporarily because of [#Coronavirus](#) you do not need to do workstation assessments”.

Special care needs to be taken in respect of employees with disabilities, as well as pregnant staff, young persons and anyone with mobility needs, with regards to work equipment and regular contact. In addition, don't forget that some staff will have limited IT skills and may struggle in this respect.

Home working can result in employees feeling isolated and regular contact with management and other colleagues should be maintained, preferably via telephone calls and video conferencing rather than e-mail. Emergency contacts and procedures should be provided. Such considerations are also important from a business continuity perspective. However, try to avoid information overload, which can lead to key messages being missed. You should also make sure that your staff keep to their set working hours and don't work for a significantly longer time than usual in the absence of clear start and end times for the working day.

Discussions between managers and employees should cover matters like mentioned above, as well as the following:

- Are specific working hours expected?
- How and where can employees be reached if they're working flexible hours?
- How should an employee communicate if they are feeling ill?
- Are any ad-hoc purchases to create a functional remote workspace reimbursable?
- A prohibition on meeting colleagues at home.

The HSE has recently updated its guidance on [lone working](#) and has guidance on homeworking [here](#).

Wellbeing

Home working can present conditions that may have a negative effect personal wellbeing and working in isolation may prove difficult to adjust to. Combining work and home can also present difficulties. Here we present some simple tips for helping your staff to adjust:

- Keep work spaces separate from areas that are usually for relaxation, such as the lounge.
- One way of alleviating the impact of home working is to relocate where work is done during the day, i.e. staff should consider moving around their home and perhaps do some working or make 'phone calls outdoors.
- Working at home with other members of the family present could mean there is additional noise and distractions and managers should consider making changes, if possible, to workload for those who are affected.
- For those who are caring for children of school age, establishing a work and/or school timetable can help to maintain some structure to the day.

- Encouraging people to take a morning walk, jog or run in the fresh air can help to set people up for the day and boost mental wellbeing. Social distancing advice just needs to be adhered to though.
- Some people relish working at home while others miss the formal work environment. Ensuring that workload and work-related activities are routinely scheduled will allow employees to see that there is some structure to the day ahead and a connection with work.
- A worthwhile approach might be to encourage colleagues to set up informal chat groups.
- Organisations should ensure ongoing access to information such as people policies, intranet sites and ways for employees to access up to date company information.

Business Continuity

Whether you're working to pre-determined business continuity plans at the moment or developing your approach "off the hoof", it is worth bearing in mind the following points:

- Your organisational priorities may be different from the ones you previously identified in the planning process and are likely to keep changing. Revisit these on a regular basis and make sure you're covering the right critical areas with the right resources (scale up, scale down).
- Have any new key person dependencies been identified during this crisis? Are these caused or affected by increased home working?
- Staff may be willing and able to support in other areas if it is safe for them to do so. This may require additional training and support.
- Check in with your key suppliers and understand their situation, which may affect you unexpectedly.
- Prepare to do an honest debrief exercise at the end of the process, including what went well, less well, lessons identified, opportunities arising etc.

Cyber Risk



There is a huge spike in the number of new users using remote services, so providing new remote access, audio video conferencing facilities and the necessary knowledge to carry out new ways of working, as well as scaling up remote access infrastructures to meet the sudden rise in demand represents key challenges for organisations.

This is also providing cybercriminals the right opportunity to play with people's fear and exploit them to their own benefits. Cybercriminals are impersonating organisations like the [World Health Organisation \(WHO\)](#) and the [US Centers for Disease Control \(CDC\)](#) by creating domain names that look similar to the official web addresses and requesting passwords and bitcoin donations to fund a fake vaccines. Individuals in the UK are getting targeted by online scammers with phishing attacks using the COVID-19 theme.

Zurich has published a paper "[The cyber dimension of the coronavirus](#)" to provide more details on the topic.

Key things to note for companies are as follows, and again it is recognised that some may be problematic in the current situation:

- Provide secure remote access infrastructure for users for home working.
- Set up an appropriate identity and access management policy ensuring that users get only the access required to carry out their work.
- Control access to corporate systems.
- Provide staff with the necessary knowledge to carry out their work on a new environment.
- Manage risk from removable media.
- Encourage users to follow appropriate cyber-hygiene.
- Educate users on being alert to fake news and fake emails.
- Report cyber-incidents to law enforcement and other regulatory bodies.
- If an employee is having internet issues at home and their service provider tells them to lower their security settings, they should consult your internal IT support department first.
- There will be IT Support challenges caused by the extra workload.
- Advise staff to shut off listening devices like Amazon's Alexa or Google's voice assistant during confidential calls and web conferences.

In the UK, the [National Cyber Security Centre](#) provides a lot of useful guidance around setting up and managing secure home working and cyber-hygiene. Finally, the Information Commissioners Office (ICO) has published their [latest advice](#) about data breach and reporting breaches under the GDPR for companies across the UK during the Coronavirus pandemic.

Data Protection

Data protection law requires organisations to make sure that personal data remains protected, whether it is being handled in an office or by an employee working from home. In addition to the possibility of data being compromised by a hacker, further risks include the possibility of data being seen by unauthorised individuals and loss of portable devices. Steps taken to secure data should be proportionate and key points to consider are:

- Ensure devices used for home working are encrypted.
- Use Information Rights Management for sensitive data. This prevents users being able to forward or print data that you have chosen to have this additional protection for.
- Remind staff on how to report a data breach.
- Make sure staff understand the rules and requirements about using personal devices for work.
- If your organisation is not yet paperless, provide staff with shredders to ensure the secure destruction of sensitive and confidential records.
- Shutting off listening devices like Amazon's Alexa or Google's voice assistant during confidential calls and web conferences is also an important consideration here.

Finally, the ICO has published their [latest advice](#) about data breaches and reporting breaches under the GDPR for companies across the UK during the Coronavirus pandemic.

Motor fleet

Given the current circumstances, we offer the following motor advice for all organisations:

- People may start using their personal vehicle for business purposes. Ensure they have appropriate business-use motor insurance and are familiar with your driver safety policies and procedures.
- Maintain regular contact with employees. They may be experiencing increased levels of stress and impairment that could adversely affect their ability to drive safely.
- Ensure that vehicle safety checks and routine servicing, maintenance and repairs continue to be carried out. Vehicles must be roadworthy or otherwise taken off the road.



- You may need to temporarily mothball vehicles on and/or off your business premises. Consider the increased risks of fire, flood, theft and vandalism and take appropriate mitigating measures.

Guidance for the transport industry on COVID-19 can be found at [GOV.UK](https://www.gov.uk), the [Fleet Transport Association](https://www.fleettransportassociation.co.uk) and the [Road Haulage Association](https://www.roadhaulageassociation.co.uk).

Some organisations with vehicle fleets will be faced with significantly increased driving hours on the part of their drivers. In this respect, the Department for Transport have announced a temporary and limited relaxation of the enforcement of [drivers' hours rules](#) in England, Scotland, and Wales for the drivers of vehicles involved in the delivery of food and certain other items.

Zurich Insurance plc Zurich Insurance plc, a public limited company incorporated in Ireland. Registration No. 13460. Registered Office: Zurich House, Ballsbridge Park, Dublin 4, Ireland. UK Branch registered in England and Wales Registration No. BR7985. UK Branch Head Office: The Zurich Centre, 3000 Parkway, Whiteley, Fareham, Hampshire PO15 7JZ. Zurich Insurance plc is authorised by the Central Bank of Ireland and authorised and subject to limited regulation by the Financial Conduct Authority. Details about the extent of our authorisation by the Financial Conduct Authority are available from us on request. Our FCA Firm Reference Number is 203093.

Communications may be monitored or recorded to improve our service and for security and regulatory purposes.

© Copyright – Zurich Insurance plc 2020. All rights reserved. Reproduction, adaptation, or translation without prior written permission is prohibited except as allowed under copyright laws.