Data Privacy Advisory Service

An Introduction to Data Protection and Working from Home

Practical tips to help when you are working from home

Introduction

Since the first lockdown in March 2020, the number of people who work from home has increased significantly. Many people who had never worked from home before were suddenly thrust into a new way of working. Furthermore, it was much easier to safeguard personal data in the office and working from home presents a new set of challenges. There are lots to consider to effectively mitigate the risk of data breaches. So, to help we have outlined our top tips for working from home.

Data Protection should be a cornerstone of of official policies, procedures and guidelines

Every employer should have a defined policy and established procedures for working from home to ensure that data is adequately protected.

Data protection should be embedded as a cornerstone of these policies and procedures. This is essential to ensure that there is an established framework to support employees as well as to ensure that as an organisation you are compliant with data protection. Data protection and working from home guidelines should be published to support staff.

Staff Awareness of Official Policies and Procedures

Clarifying the expectations that employers have, will help remind employees of what the appropriate guidelines are to follow while they are working from home and ensures everyone is on the same page. These policies and procedures will not be effective if they are not appropriately communicated.

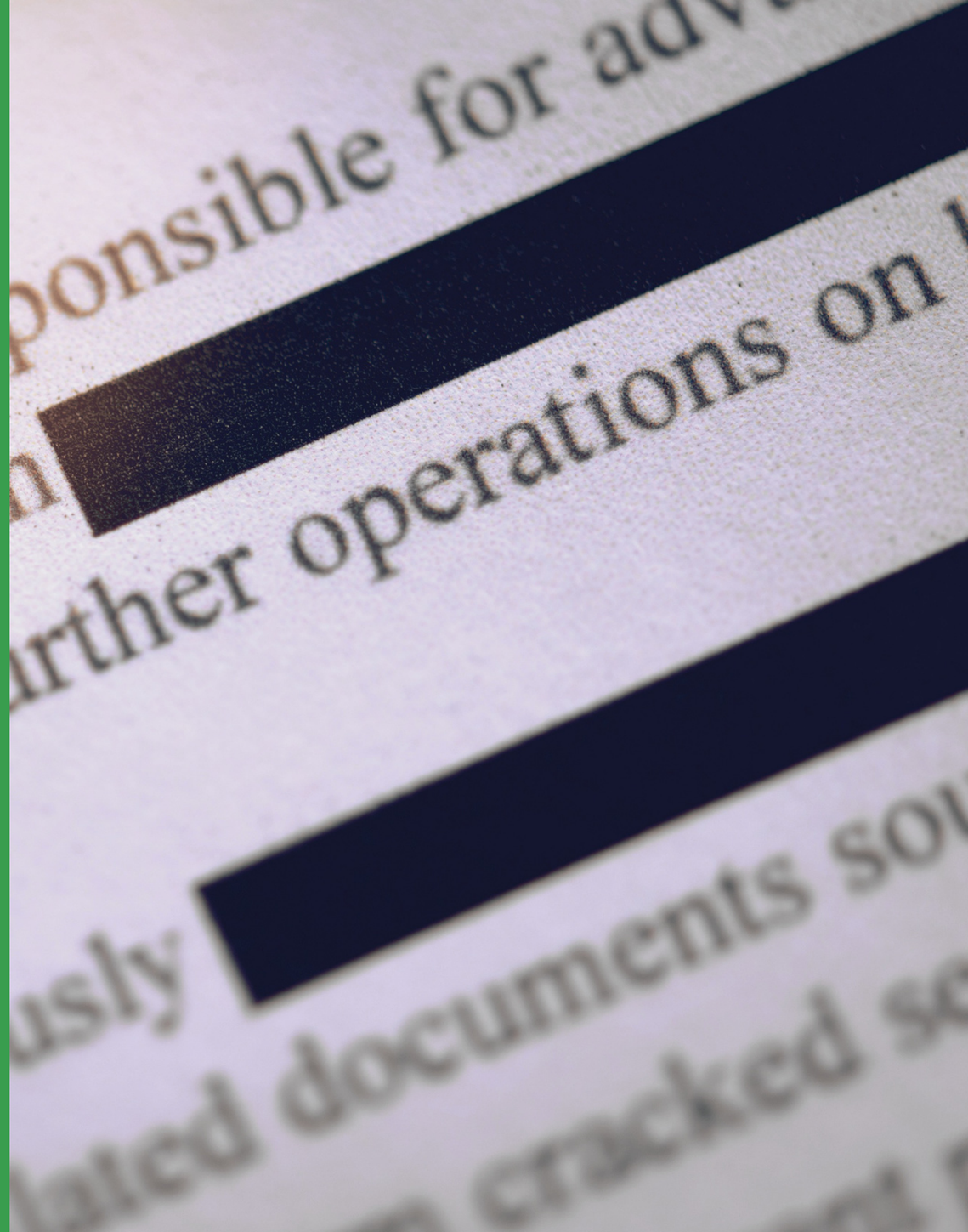
Employees should be regularly reminded of these policies and procedures to ensure that everyone is working to the same standards i.e., not taking shortcuts and using unapproved methods of communication which could put personal data at risk.

Keep Data Secure

Employees should only use approved technology when handling personal data and conducting work-related tasks. Every device that employees use should be fitted with the approved software that has been checked to ensure it is providing the best protection for personal data. Employees should never send emails through their personal accounts or use unapproved software for different forms of communication.

If employees are using devices that have been issued by their employer, the employer has a duty to ensure that the devices can be securely supported and updated remotely. Furthermore, employers should ensure that mechanisms and checks are in place to prevent external data breaches from third parties.

Keep software updated and separate



Employees should ensure that the devices and software they are using for work is kept up to date and secure by conducting regular checks on their operating systems and software for any potential security concerns.

It is key that employers provide appropriate anti-virus software for employees to use. Employees should be regularly reminded to never open unverified links or attachments.

Filing Systems and Storage

Employers should create and implement protocols on the management of the organisation’s data by ensuring that the device owner’s data and the organisation’s data are kept separate. Staff should be reminded not to move the organisation’s data into their personal storage or onto separate personally owned devices.

Furthermore, staff should follow the organisation’s policies to safely process print outs and all work-related paper and devices should be locked away at the end of the working day if possible. This is key to avoiding the loss or theft of personal data.

Layers of Security

In this ever-evolving connected world, it is now easier than ever for anyone to gain unauthorised remote access to your accounts and devices. It is key that everyone remains vigilant with their password security. The National Cyber Security Centre recommends that everyone should use a three-word passphrase instead of a password as part of their #thinkrandom campaign. And ensure that you use different passwords for different accounts to improve your cyber security.

In addition, employers should consider implementing multi-factor authentication to keep devices safe such as two-factor authentication to support password security. Consider another layer of security by encrypting documents with passwords and sending the password by another method, or by using an encrypted email provider such as Egress.

Have you got the tools you need to work effectively from home?

It is a legal requirement for employers to ensure that their employees have all the resources they need to work. (This legal requirement is the Health and Safety (Display Screen Equipment) Regulations 1992 as amended by the Health and Safety (Miscellaneous Amendments) Regulation 2002.)

Many people do not have the resources at home that they did in the office such as an additional monitor (second screen), keyboard or mouse that is integral to office work. Not having the appropriate resources, can lead to poor productivity, data breaches, and other consequences. Therefore, it is essential that every employee conducts a Display Screen Equipment (DSE) assessment for their home office as well.

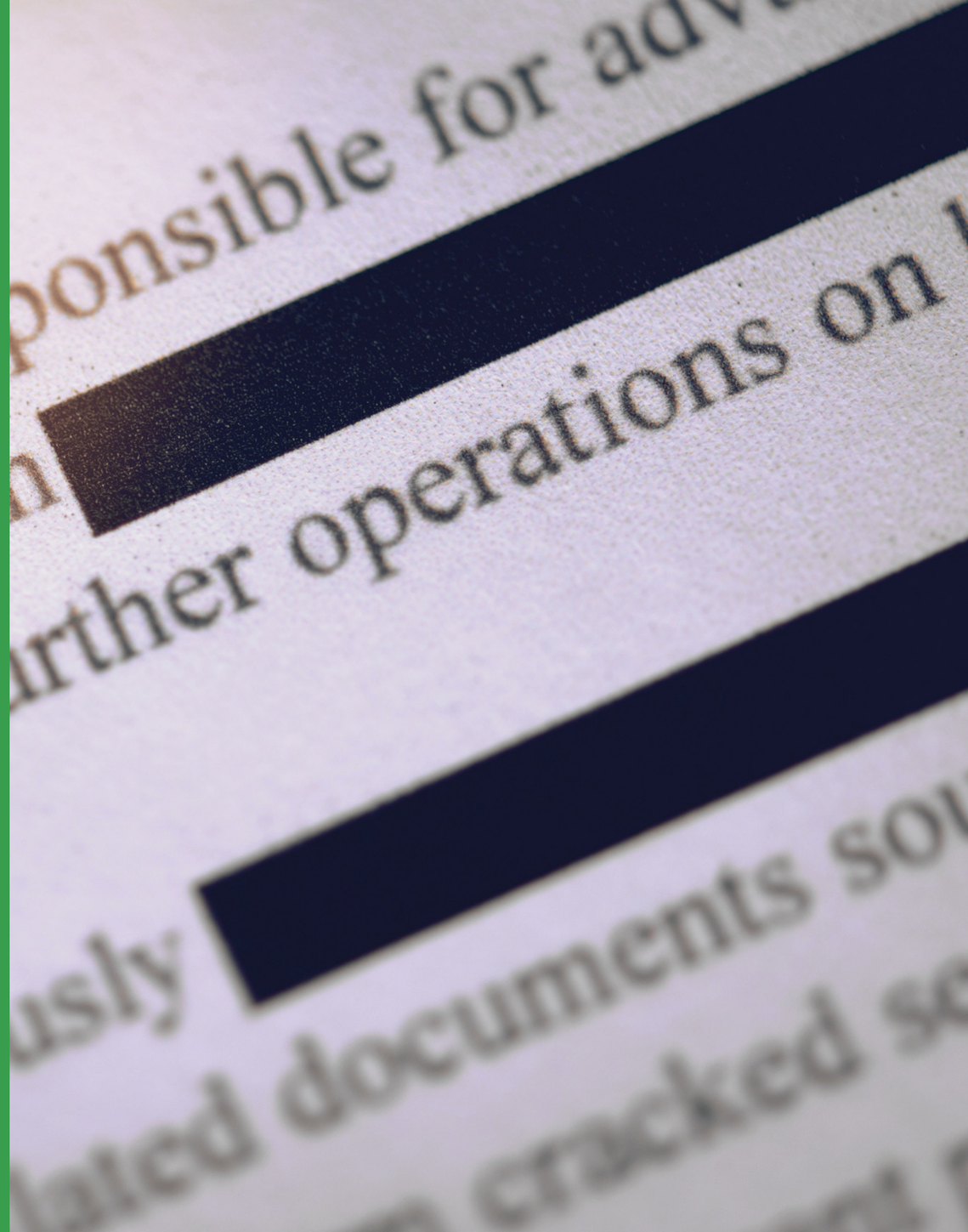
Communication

Effective, safe communication is critical to the efficiency of organisations, so approved secure messaging apps, online document sharing systems need to be put in place to help employees safely share data. Since working from home can be very isolating, it is key to ensure that staff are supported.

Consider having a group chat with each team where everyone can touch base with each other at the start and end of each day. This group chat can be used to ensure everyone’s wellbeing and to distribute the workload appropriately.

Additionally, check that the Wi-Fi connection you are using is secure and password protected.

Define and establish boundaries



It is recommended that you should create a dedicated office space in your home so when you close that laptop at the end of the working day you can create some space between work and your home life.

An acceptable work environment should be defined in the official working from home policies and procedures. This is also integral to ensuring that employees are working in an environment where they are ensuring that the personal data, they are processing is not accessible by anyone else in their home environment.

Employees should be reminded to always maintain confidentiality.

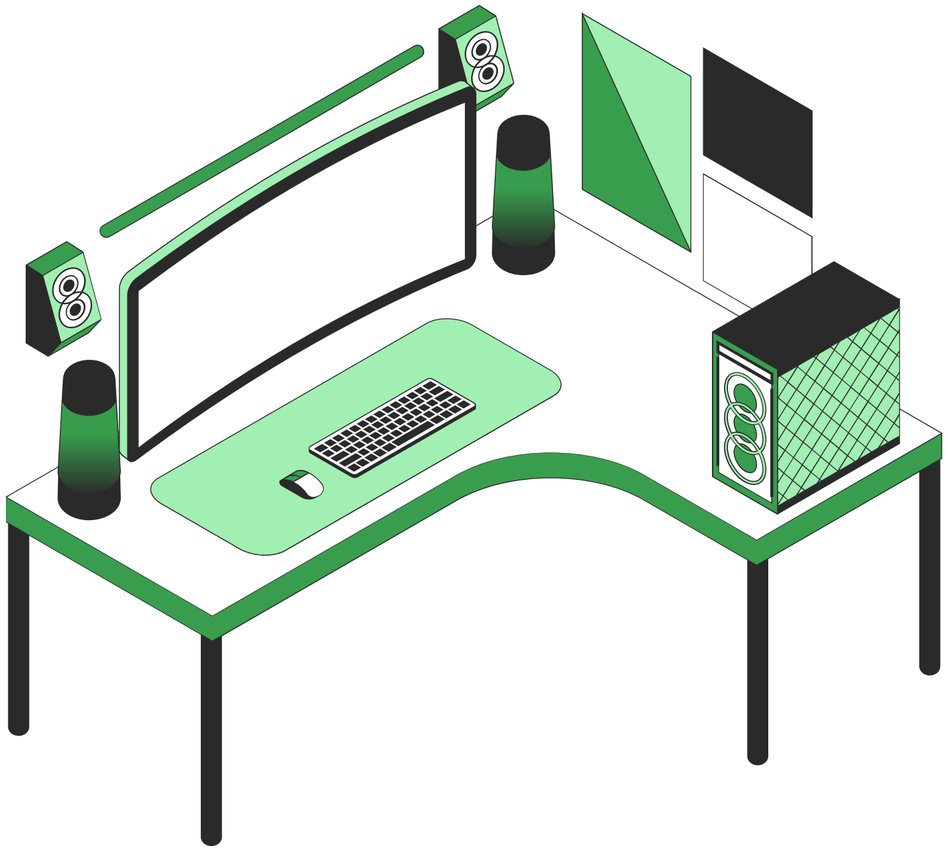
Consider staff wellbeing

Many data breaches occur when staff are distracted, stressed or forget to follow established processes due to time pressure. Therefore, it is key that everyone is encouraged to take regular breaks.

Advise taking a quick walk outside to get some fresh air or making a cup of tea and switching off for ten minutes. Staff should break up tasks into manageable chunks where they can completely focus on each task and not get distracted by other pieces of work.

Additional points to consider

- To protect your wellbeing, consider turning off your work-related notifications from your laptop, mobile phone when you are no longer on the clock. This is key if you are using these devices for both work and personal use.
- Check if your employer offers discounts on eye tests before your book your eye test if your eye test is covered under occupational health.
- The government's Health and Safety Executive offers a free template on how to conduct a DSE assessment (https://www.hse.gov.uk/pubns/ck1.pdf).
- Multi-factor authentication is key to improving access control and strengthening cyber security by mitigating the risk of unauthorised access by individuals.



Do you have any questions?

There are many factors to consider when employees are working from home, and this list is not exhaustive. However, it is a good starting point to consider improving your data strategy now that more employees are working from home.

For further information on how we can help improve your data strategy and compliance within your organisation, get in touch with the DPAS team.

www.dataprivacyadvisory.com
info@dataprivacyadvisory.com