TOP 8 TIPS FOR HOME WORKING

1 ADHERE TO POLICIES & PROCEDURES

Follow company data protection and information security policies, procedures, and guidelines as normal. Avoid sending emails through your personal account or using the video conferencing app that you use with friends, for work related calls.

2 APPROVED TECH ONLY

Use company-owned technology only when working with personal data. This provides the best protection, even if personal technology might seem more convenient.

3 TAKE CARE WITH PRINT-OUTS

Be careful with print-outs of personal data. Dispose of them carefully if you do not have a shredder at home. Try to avoid mixing work print-outs with home print-outs or leaving them on the home printer. If necessary, keep all paper records together and destroy them securely when you can return to the office.

4 LOOK OUT FOR PHISHING ATTACKS

There has been a big spike is phishing emails during lockdown. These often look like a genuine emails. Be extra vigilant about opening web links and attachments in emails or other messages. If you were not expecting the message, then do not open the attachment or click the link – call the sender or IT to check first. This includes any messages claiming to provide COVID updates.

evalian

5 SEPARATE DATA

Do not mix company data with home-related data. This includes print-outs and data on devices such as external storage or computers. Do not use personal computing devices for work purposes.

6 LOCK AWAY PRINT OUTS & DEVICES

At the end of each day, secure devices and paper records containing personal data in a secure location – such as a lockable drawer where possible.

CONFIDENTIALITY

Try to hold conversations where others are less likely to overhear you and position your screen where it is less likely to be seen. If you have a Smart device (Alexa, Google smart speakers) in your work space, you should consider turning off the microphones.

USE SECURE COMMUNICATION METHODS ONLY

Use only company-approved communication methods. It can be tempting to try Zoom, Google Hangouts or other video and collaboration tools but these can present security and data protection risks and should only be used if approved. Encrypt or password protect any personal data you need to share by email and/or use secure file sharing on SharePoint. Remember to send passwords using a different communication method, such as by text.

evalian